ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Кабанов Я. В.
(прізвище та ініціали)
Керівник Гахов С. О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ABAC – Attribute-Based Access Control

ACL – Access Control List

ACM – Access Control Mechanism

API – Application Programming Interface

AWS – Amazon Web Services

IAM – Identity and Access Management

SSO – Single Sign-On

ВСТУП

Актуальність дослідження. Сьогодні в сучасних організаціях широко застосовуються веб-додатки, які входять до складу їх інформаційних систем. Вразливості веб-додатків експлуатуються зловмисниками для досягнення різних злочинних цілей, що ще більш загострює проблему забезпечення кібербезпеки інформаційних систем організацій.

Сучасні організації широко використовують у своїй роботі багато різних програм, у тому числі класичні десктопні, мобільні та веб-додатки. Вони можуть бути розгорнуті на серверах організації або бути хмарними сервісами. Кожен додаток вимагає вирішення завдання управління доступом, а користувач змушений запам’ятовувати паролі від всіх його облікових записів і знову проходити ідентифікацію/автентифікацію. Зі зростанням числа використовуваних додатків та розвитком проблем забезпечення доступу користувачів виникає потреба в централізованому управлінні доступом.

Технології управління доступом користувачів (Identity and Access Management, IAM) надають всім додаткам організації єдиний сервіс управління ідентифікацією, що спрощує життя користувачів та підвищує безпеку систем. Щоб уникнути поширених помилок (наприклад, впровадження перевантажених технологій і, як наслідок, суттєвої витрати ресурсів), починати побудову системи управління доступом в організації слід саме з впровадження сервісів IAM.

В роботі проаналізовано проблему управління доступом користувачів до хмарних сервісів та ресурсів організації та визначено його мету та завдання. Проведено аналіз існуючих технологій управління доступом користувачів до хмарних сервісів та ресурсів організації. Досліджено методи та засоби управління доступом користувачів до сервісів та ресурсів Amazon Web Services. Визначено призначення, основні функції та склад рішення AWS IAM.

На основі досліджень проведених в роботі запропоновано порядок застосування технології управління доступом користувачів до сервісів та ресурсів AWS організації. Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології застосування технології управління доступом

користувачів до хмарних сервісів та ресурсів організації.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження щодо технології управління доступом користувачів до сервісів та ресурсів Amazon Web Services.

Об'єкт дослідження – процес управління доступом користувачів до сервісів та ресурсів організації.

Предмет дослідження – технологія управління доступом користувачів до сервісів та ресурсів Amazon Web Services.

Мета роботи – розробити порядок застосування технології управління доступом користувачів до хмарних сервісів та ресурсів організації та рекомендації щодо його реалізації.

Наукові завдання:

дослідити сутність проблеми забезпечення доступу користувачів до хмарних сервісів та ресурсів організації;

встановити сутність завдань управління доступом користувачів до хмарних сервісів та ресурсів організації;

проаналізувати існуючі технології управління доступом користувачів до хмарних сервісів та ресурсів організації;

проаналізувати методи та засоби управління доступом користувачів до хмарних сервісів та ресурсів організації;

проаналізувати основні функції та принципи реалізації управління доступом до хмарних сервісів та ресурсів організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління доступом користувачів до сервісів та ресурсів AWS організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2021 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ХМАРНИХ СЕРВІСІВ ТА РЕСУРСІВ ОРГАНІЗАЦІЇ

1.1. Дослідження можливостей застосування хмарних сервісів та ресурсів в сучасних організаціях

Згідно з дослідженнями компанії RightScale, за останні три роки частка бізнесів, що використовують хмарні сервіси, зросла з 89% до 92%. Зараз понад 80% організацій, що мають 1000 або більше працівників, використовують одночасно декілька хмарних платформ. Очікується, що до 2024 року цей показник зросте до 90%. Більше того, прогнози свідчать, що упродовж наступного року витрати бізнесу на публічні хмарні платформи сягнуть $277 млрд, що на 73% більше, ніж у 2018 році. А загальний обсяг ринку хмарних сервісів має досягти показника у $350 млрд у 2022-му [4].

Ще десять років тому організації переважно використовували власні, локальні центри обробки даних (ЦОД), які потребують великої кількості ресурсів та фахівців. Зі зростанням складності ЦОДів та кількості залучених фахівців, необхідних для управління ними, витрати на IT стали проблемою для багатьох організацій.

Проблема багато в чому вирішилася з появою хмарних технологій. Ключові переваги, які організації можуть очікувати від застосування хмарних сервісів:

ефективність/зниження витрат. Використовуючи хмарну інфраструктуру, організаціям не потрібно витрачати гроші на покупку та обслуговування обладнання. Організаціям не знадобиться команда IT фахівців для керування хмарною інфраструктурою, оскільки нею може керувати хмарний провайдер;

безпека даних. Одне з основних завдань будь-якого бізнесу, незалежно від розміру та галузі, є забезпечення безпеки даних. Наприклад, несанкціонований доступ до даних організації може підірвати лояльність клієнтів, позиціонування бренду та призвести до збитків. Хмара пропонує багато розширених функцій

безпеки, які гарантують надійне зберігання та обробку даних;

адаптивність. У різних організацій різні потреби в технологіях – велике підприємство з більш ніж 1000 співробітників та стартап потребуватимуть різного обсягу обчислень та кількості обладнання. Хмарні рішення підходять для організацій із зростаючими або змінними вимогами. Якщо потреби організації зростають, можна збільшити ємність хмари, не вкладаючи коштів у фізичну інфраструктуру. Такий рівень гнучкості може дати організаціям, які використовують хмарні обчислення, реальну перевагу перед конкурентами;

мобільність. Хмарні обчислення забезпечують постійний доступ до корпоративних даних через смартфони та інші пристрої. Так співробітники в офісі або працюючі віддалено зможуть підтримувати зв'язок із клієнтами та колегами 24/7, а також отримувати доступ до своїх документів з будь-якого пристрою.

аварійне відновлення Втрата даних є серйозною проблемою для всіх організацій. Зберігання даних у хмарі гарантує, що вони будуть завжди доступні, навіть якщо обладнання, ноутбуки чи ПК пошкоджено. Хмарні послуги забезпечують швидке відновлення даних за всіма видам надзвичайних ситуацій – від стихійних лих до відключення електроенергії.

Необхідно підкреслити, що хмарні сервіси – це зручне рішення для сучасних організацій, що орієнтуються на міжнародний ринок. Хмарні послуги там можуть забезпечувати безперервну підтримку найважливіших бізнес-операцій або стати запасним сховищем для корпоративних даних.

Основні переваги використання хмарних сервісів для організацій:

надійність та життєздатність: розподіл даних по ЦОДах у різних географічних місцях забезпечує їх збереження у разі збоїв та надзвичайних подіях, які порушують роботу дата-центру у конкретному місті;

доступність: європейські та американські провайдери надають світовий рівень якості обслуговування, при цьому за доступною для замовників ціною, що нерідко може бути вигіднішим за аналогічні пропозиції локальних провайдерів;

найновіші технології та обладнання: великі хмарні провайдери за використовують Hi-End обладнання. Наприклад, сервери Cisco та сховища

NetApp.

Багато організацій активно переходять на хмарні обчислення, тому що це дозволяє їм бути гнучкими та конкурентоспроможними в умовах швидких змін клієнтів. Хмара сприяє постійному вдосконаленню бізнесу, допомагає стандартизувати заходи безпеки [4].

Різноманіття хмарних технологій сьогодні дозволяє задовольнити вимоги організації будь-якого розміру. Існує три основні типи хмар, в залежності від того, де розташовані сервіси та як їх розгортають [4]:

приватна хмара. Вона доступна через захищену мережу для однієї організації. Приватну хмару можна розмістити на своїй території або віддати на аутсорсінг сторонньому провайдеру. Її головні переваги: висока видимість, можливість персоналізації (налаштування під свої потреби), першокласна безпека та контроль, висока гнучкість та масштабованість. Недоліки: висока ціна (це може бути серйозною перепоною для малого та середнього бізнесу) та складність в обслуговуванні (можуть знадобитися окремі працівники для технічної підтримки приватної хмари);

публічна хмара. Постачальник таких послуг пропонує їх багатьом користувачам одночасно. Також провайдер самостійно виконує технічну підтримку, дбає про «залізо» та програмне забезпечення. Завдяки цьому публічна хмара обходиться клієнтам набагато дешевше, аніж приватна, економить час та кошти, дозволяє бізнесу сфокусуватися на своїх головних завданнях. З іншого боку, вона більш вразлива до кібератак і має обмежені можливості персоналізації;

гібридна хмара. Вона є комбінацією приватних та публічних хмарних рішень. Зазвичай її ресурси інтегровані в унікальне середовище і розподілені між хмарами, щоб забезпечити максимальну продуктивність. Гібридна хмара відкриває майже безмежні можливості для IT-менеджерів. Приватна її складова гарантує безпеку, а публічна – допомагає керувати допоміжними бізнес-додатками на кшталт HRM, CRM, електронної пошти. Недоліком гібридної хмари є певна складність інтеграції приватної та публічної хмар – для цього потрібна професійна команда IT-експертів. Крім того, складність інфраструктури може

часом призводити до локальної неефективності.

Тим не менше, дедалі більше компаній віддають перевагу саме гібридній хмарі, зокрема медичні установи, юридичні та фінансові організації. Це дозволяє їм, поміж іншого, безпечно ділитися даними з третіми особами [4].

Другий новітній підхід – мультихмарне рішення: використання декількох хмар, але без розподілу даними між ними. Популярність цієї нової IT-архітектури теж зростає, оскільки вона пропонує доступ до декількох сервісних моделей одночасно. За прогнозами компанії Gartner, у 2021 році 75% великих та середніх організацій використовуватимуть саме гібридний або мультихмарний підхід [4].

Компанія Gartner [5] зазначає, що ринок хмарної інфраструктури та платформних сервісів консолідується – понад 90% світового ринку зосереджено лише у чотирьох хмарних провайдерів: Amazon Web Services та Microsoft лідирують на ринку, а Alibaba та Google є найближчими конкурентами.

Ця консолідація не показує жодних ознак уповільнення. AWS і Microsoft продовжують домінувати здебільшого у Північній Америці та Європі, де загальні темпи зростання хмарних технологій залишаються високими. Alibaba – домінуюча сила в Китаї та серйозний конкурент у країнах, де Китай має вплив [5].

Однак епоха китайського провайдера послуг лише починається [5]. Такі провайдери, як Alibaba Cloud, Tencent, Huawei та Kingsoft, виявляють великий інтерес до конкуренції не тільки на регіональному рівні в Азії, але й у віддалених регіонах, таких як Латинська Америка, де китайські провайдери стикаються з менш ворожим прийомом, ніж на Заході [5].

Глобальна консолідація відбувається в основному внаслідок того, що підприємства шукають промислові пропозиції, які несуть із собою рівень надійності та широкий спектр функціональних можливостей для задоволення всіх робочих навантажень підприємства. Це ключова відмінність між всесвітнім постачальником та регіональним постачальником, який може мати віртуалізовану пропозицію, що складається з обчислень, мережі та сховища з використанням готових продуктів віртуалізації. Регіональні провайдери просто не в змозі конкурувати зі швидкістю інновацій світових провайдерів [5].

1.2. Аналіз проблеми забезпечення безпеки хмарних сервісів та ресурсів

Прискорення розвитку цифрового бізнесу стимулює інвестиції в нові архітектури та створює нові проблеми управління ідентифікацією та доступом (IAM). Тепер кожна організація сфокусована на прагненні цифрової трансформації та необхідності адаптуватися до стрімких технологічних, організаційних та соціальних змін.

За визначенням Gartner *управління ідентифікацією та доступом (IAM)* – це дисципліна, яка дає змогу потрібним особам отримувати доступ до потрібних ресурсів у потрібний час з потрібних причин. IAM вирішує критично важливу потребу в забезпеченні належного доступу до ресурсів у дедалі гетерогенних технологічних середовищах і для забезпечення все більш суворих вимог до відповідності. IAM є важливою справою для будь-якого підприємства. Це все більше пристосовується до бізнесу, і для цього потрібні ділові навички, а не лише технічні знання. Підприємства, які розробляють зрілі можливості IAM, можуть знизити витрати на управління ідентифікацією та, що ще важливіше, стати значно більш гнучкими у підтримці нових бізнес-ініціатив.

Програми управління ідентифікацією та доступом (IAM) надають керівникам безпеки та ризиків ретельну практику, процеси та технології для керування ідентифікаторами та правами людей, послуг та речей. Ці програми також охоплюють відносини та довіру між цими людьми, послугами та речами. У сучасному складному та розподіленому IT-середовищі сучасні програми IAM повинні робити набагато більше, ніж просто надавати ідентифікатори користувачів і надавати доступ [8].

Програми IAM є основою досягнення найважливіших бізнес-цілей і актуальними для кожної високопродуктивної організації. Як наслідок, лише деякі ініціативи в галузі IT або безпеки потребують такого обговорення та ретельного аналізу, як IAM. Сучасна програма IAM виходить за рамки встановлених інструментів і зосереджується на результатах та усуненні технічної

заборгованості або важких налаштувань, які заважають організації розгортатися в масштабі [8].

Сучасні програми IAM зміщують фокус з тактичних або ручних операцій на більше стратегічні функції, оптимізовані для цілей бізнесу. Крім того, відмінні риси модернізованої програми IAM можуть допомогти зменшити ризик злому даних, пов’язаних із ідентифікацією та обліковими даними. Ці програми можуть допомогти підвищити продуктивність і співпрацю, забезпечуючи конкурентну перевагу на ринку. Нарешті, сучасна програма може допомогти забезпечити більш систематичне забезпечення та підтримку управління дотриманням нормативних вимог, одночасно зменшуючи витрати на виправлення висновків аудиту за участю IAM.

Багато підприємств, які прагнуть до цифрової трансформації, вважають, що програми IAM є ключовими для цієї ініціативи змін. Стратегії оптимізації цифрової трансформації включають модернізацію інструментів на робочому місці, міграцію в хмару, інтеграцію програмного забезпечення як сервісу (SaaS) і локальних додатків, ініціативи роботи з дому та розширення каналів залучення клієнтів. Ці імперативи можуть забезпечити визнану цінність бізнесу та конкурентну перевагу. Аналогічно, IAM має значну можливість надати пряму цінність бізнесу, забезпечуючи меншу вартість, керовану ризиками взаємодію з постачальниками, партнерами та клієнтами та допомагаючи покращити загальний досвід користувачів і клієнтів.

Програми IAM дозволяють кінцевим користувачам, зацікавленим сторонам, постачальникам безперешкодно, швидко та ефективно отримувати доступ до ресурсів, так що потрібний користувач отримує правильний доступ до потрібних захищених ресурсів за належних умов.

Але багато організацій не можуть досягти однієї або кількох із цих цілей через фрагментовані, застійні та неповні програми IAM, які були розроблені з часом з використанням монолітних точкових технологічних рішень. В результаті підприємства стикаються зі значними ризиками невдач і можуть втратити конкурентну перевагу гнучкої та пов’язаної робочої сили [8].

Традиційні програми IAM також стикаються з наступним тиском [8]:

велика складність – компанії зазвичай додають більше додатків, інформації, методів доступу та прав користувачів за потреби;

більше зосередженості на користувачеві – збільшення очікувань щодо захисту персональної інформації (PII) та забезпечення безперебійної роботи користувача;

більше регулювань – нові стандарти, що розвиваються, необхідні для доступу та обміну ідентифікаційною інформацією та конфіденційною інформацією;

більше інструментів безпеки – в середньому організації використовують від 25 до 49 різних інструментів безпеки від 10 різних постачальників.

Продуманий підхід до модернізації існуючої програми IAM може призвести до переваг, які безпосередньо покращують ефективність бізнесу та безпеку, як-от такі результати [8]:

зниження витрат за рахунок автоматизації;

забезпечення операційної ефективності для людей і систем за допомогою інтегрованої технологічної структури;

допомога підтримати більш успішне впровадження шляхом належного планування;

покращення аналізу ризиків;

зниження вартості відповідності;

підвищення досвіду клієнтів і співробітників.

Програма IAM, оптимізована для задоволення потреб і унікальних обставин організації, допомагає розширити можливості управління дотриманням нормативних вимог, надає зручний доступ авторизованим користувачам і захищає цінні дані. Але без використання сучасної програми IAM бізнес може зіткнутися з такими значними перешкодами [8]:

доданий час і витрати на ручні процеси IAM;

поганий досвід користувачів;

відсутність навичок розгортання сучасних рішень;

висока технічна заборгованість з монолітними налаштуваннями;

погані інновації та продуктивність працівників.

Потенційне зростання витрат також є фактором, який особливо турбує підприємства, які не мають сучасної програми IAM. Згідно зі звітом Ponemon про вартість внутрішньої загрози за 2020 рік, найдорожчою інсайдерською загрозою за кожен інцидент є крадіжка облікових даних [8].

Частота та вартість цих інцидентів значно зросла. Фактично, частота інцидентів на компанію з 2016 року зросла втричі з 1 до 3,2, а середня вартість майже подвоїлася з 493 093 доларів США за той же період [8].

$871 тис. – середня вартість за випадок крадіжки облікових даних для підприємств у 2019 році за даними [8].

Для організацій, які хочуть підвищити точність і швидкість надання доступу до потрібної особи в потрібний час за належних умов, потреба в сучасній програмі IAM є першочерговою. Але існують і інші вагомі причини для впровадження, які також мають враховувати керівники з безпеки та IT на підприємствах.

Керівники служб безпеки та управління ризиками стикаються з повсюдними збоями у рішеннях управління ідентифікацією та доступом (IAM) з багатьох причин, в першу чергу через зростання прагнення до взаємодії з клієнтами по цифрових каналах та раптового та швидкого розширення віддаленої робочої сили через пандемію [9].

До 2025 року сітка кібербезпеки підтримуватиме більше половини всіх запитів IAM, що дозволить створити більш явну, мобільну та адаптивну уніфіковану модель управління доступом. Коміркова модель кібербезпеки забезпечує більш інтегрований, масштабований, гнучкий і надійний підхід до управління доступом до цифрових активів, ніж традиційні засоби контролю периметра безпеки [9].

Через значне збільшення кількості віддалених взаємодій із співробітниками настійно необхідні надійніші процедури реєстрації та відновлення, оскільки важче відрізнити зловмисників від законних користувачів. До 2024 року 30% великих

підприємств впроваджуватимуть нові інструменти захисту особистості для усунення поширених недоліків у процесах життєвого циклу ідентичності персоналу [9].

1.3. Аналіз моделей, методів та засобів управління доступом користувачів до хмарних сервісів та ресурсів

Аналіз існуючих рішень кібербезпеки на макрорівні показує, що кожне з них потрапляє в одну з трьох логічних груп, які показано на рис. 1.1 [1].

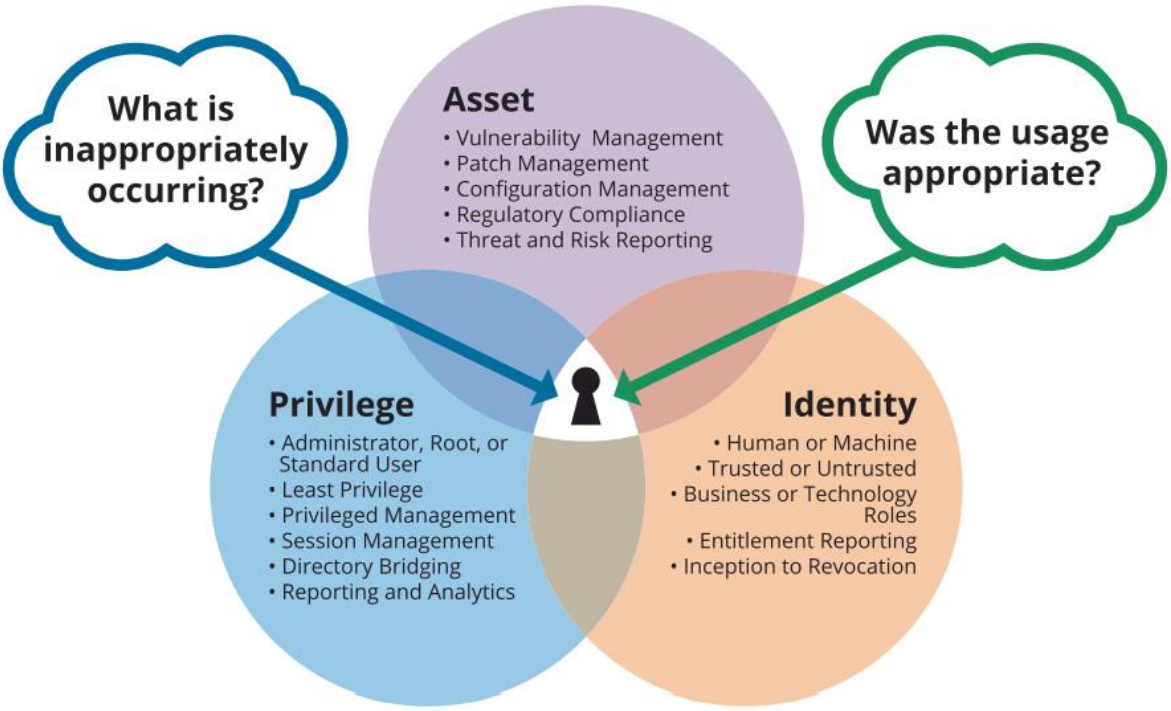

Рис. 1.1. Три основних групи рішень з кібербезпеки [1]

Основні рішення з кібербезпеки можна охарактеризувати як [1]:

ідентифікація – захист особи, облікового запису та облікових даних користувача від неналежного доступу;

привілеї – захист прав, привілеїв та контролю доступу для особи або облікового запису;

актив – захист ресурсу, який використовується ідентифікатором, безпосередньо або як послуга.

Розглянемо основу корпоративного IAM.

Існує безліч платформ, які допоможуть вам визначити, організувати, реалізувати та покращити безпеку. Такі ініціативи, як «Цілі контролю за інформаційними та суміжними технологіями» (Control Objectives for Information and Related Technology, COBIT), Структура кібербезпеки Національного інституту стандартів та технологій США (National Institute of Standards and Technology, NIST) та Міжнародна організація зі стандартизації (International Organization for Standardization, ISO) серії 27K – всі вони забезпечують основи для управління безпекою [1].

Одна з найсерйозніших проблем, з якими стикаються всі системи безпеки, – їхня складність. Управління ідентифікацією є частиною більшості, якщо не всіх, офіційних підходів до забезпечення безпеки. Управління ідентифікацією розглядається як набір універсальних принципів, які застосовуються до всіх встановлених структур безпеки та практично до всіх сценаріїв безпеки підприємства [1].

Управління ідентифікацією базується на автентифікації, авторизації, адмініструванні, аудиту та аналітиці (рис. 1.2).

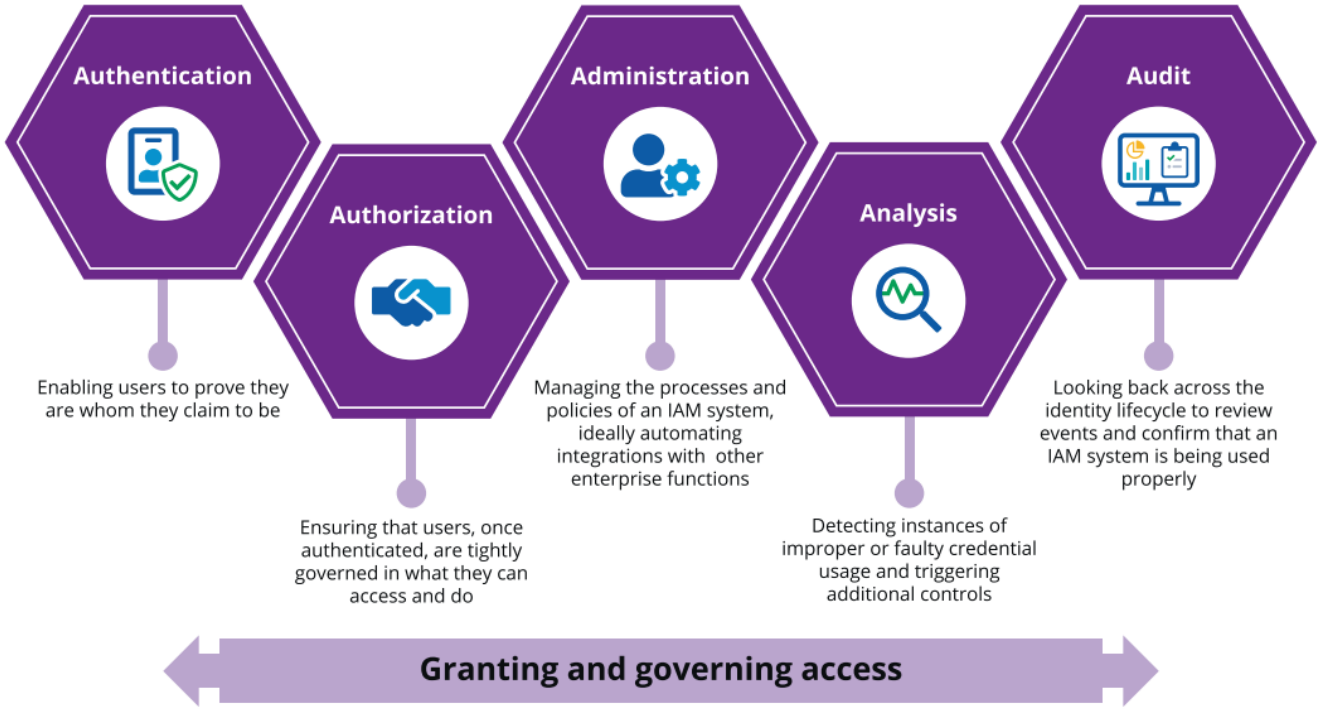

Рис. 1.2. Основа управління ідентифікацією [1]

Автентифікацію часто плутають з авторизацією, хоча це різні технології та практики. У деяких обчислювальних моделях автентифікація та авторизація змішуються разом і не мають особливої різниці чи поділу в реалізації чи управлінні. Apple iOS, наприклад, використовує біометричні дані як для авторизації, так і для автентифікації, і доступ кінцевого користувача розмивається незалежно від типу дії. За визначенням, автентифікація – це логін (ім'я користувача) на додаток до певної форми секрету, історично паролю, для встановлення доказу або довіри до особистості. По суті, це підтвердження того, ким ви себе називаєте [1]. Формула автентифікації:

Authentication of your identity = login + shared secret (password).

Хоча існує незліченна кількість варіантів спільних секретів, які можна використовувати під час входу, таких як пін-коди, паролі, ключі, двофакторна автентифікація тощо, сам логін, як правило, не є секретом і часто можна вгадати для ідентифікації. Однак логін також може бути чимось складнішим, як-от номер співробітника, який краще маскує особистість користувача. Для високозахищених середовищ цей другий підхід є кращим, особливо для облікових записів адміністратора або root. Ви не можете візуально ідентифікувати привілеї облікового запису, просто подивившись на обліковий запис або ім'я користувача. Отже, автентифікація – це не що інше, як підтвердження особи чи права власності на певний обліковий запис. Він не надає дозволів, привілеїв чи доступу, лише підтвердження того, що особа є тією, ким є [1].

Авторизація є наступним кроком після автентифікації. Особа не можете бути уповноваженою виконувати функцію, призначати привілеї чи навіть виконувати завдання у певній ролі без попередньої автентифікації. Формула авторизації:

Authorization = privileges (what you are allowed to do) + authentication.

Таким чином, авторизація – це право виконувати функцію на основі автентифікації. Особі та пов'язаному з нею обліковому запису надаються привілеї для виконання певних функцій, а також можуть бути явно відмовлені чи не привілейовані для виконання інших функцій. Ці привілеї можуть бути призначені

в програмі, операційній системі або деякій частині допоміжної інфраструктури. Його також можна призначити в системі керування ідентифікацією або привілеями, яка його контролює [1].

Коли подібні привілеї згруповані разом, вони створюють основу ролі. Коли групі облікових записів призначається роль, вона надає цій групі дозвіл на виконання цих функцій. У разі мобільного пристрою, такого як Apple iPhone, що працює під керуванням iOS, розпізнавання обличчя або дотик відбитків пальців використовуються як для автентифікації, так і для авторизації [1].

Сьогодні використання одного і того ж механізму або техніки для автентифікації та авторизації одночасно може призвести до значних проблем, пов’язаних із цілісністю, контролем та наглядом за процесом, і багато хто в галузі зараз вважають, що їх слід виконувати окремо. Порушення або слабкість в одній моделі призводить до порушення або слабкості в іншій. Навіть у «найсучасніших» обчислювальних середовищах ми часто бачимо ту саму відсутність поділу, коли рішення єдиного входу (SSO) стирає межу між початковою автентифікацією та автоматичною авторизацією в межах керованої програми. Рішення багатофакторної автентифікації (MFA) можуть допомогти зменшити цей ризик, вимагаючи повторної перевірки для привілейованої авторизаційної діяльності [1].

Адміністрування тут означає керування конфігурацією та контроль за будь-якими змінами, внесеними до цієї автентифікації, авторизації та аудиту. Більшість організацій все ще намагаються отримати повний адміністративний контроль над системами та даними, за захист яких вони відповідають. Тому, на нашу думку, важливо, щоб адміністрування розглядалося незалежно від постійно мінливого поєднання технологій AuthN (автентифікація) та AuthZ (авторизація) [1].

Мета проведення *аудиту* є довести, що комплексні адміністративні процеси та політика діють і дотримуються.

Аналітика означає отримання інформації про роботу та безпеку шляхом постійного збору й обробки даних про конфігурацію, призначення та використання ідентифікаторів. Розширена аналітика ідентифікації забезпечує більш обґрунтований та прогнозований підхід до управління. Використовуючи

методи машинного навчання (ML) і штучного інтелекту (AI), інструменти аналізу ідентифікації можуть надати важливу інформацію для аналізу, яка допомагає розширити функції аудиту і адміністрування ідентифікацією та зробити їх більш динамічними та чутливими [1].

Співробітники, підрядники та ділові партнери потребують доступу до корпоративних систем і даних. Розуміння того, хто має доступ, хто повинен мати доступ і як цей доступ використовується, є важливою проблемою безпеки бізнесу та IT.

Управління ідентифікацією (Identity Governance) став найважливішим будівельним блоком в автоматизації корпоративних інформаційних технологій, безпеці підприємства та корпоративному управлінні відповідністю. Воно забезпечує основу контролю доступу користувачів і, зрештою, допомагає знизити загальний операційний ризик [1].

Identity Governance – це технологія та процеси, що забезпечують людям відповідний доступ до додатків та систем, а також для організації забезпечити знання того, хто до чого має доступ, як цей доступ можна використовувати і чи відповідає цей доступ політиці (рис. 1.3) [1].

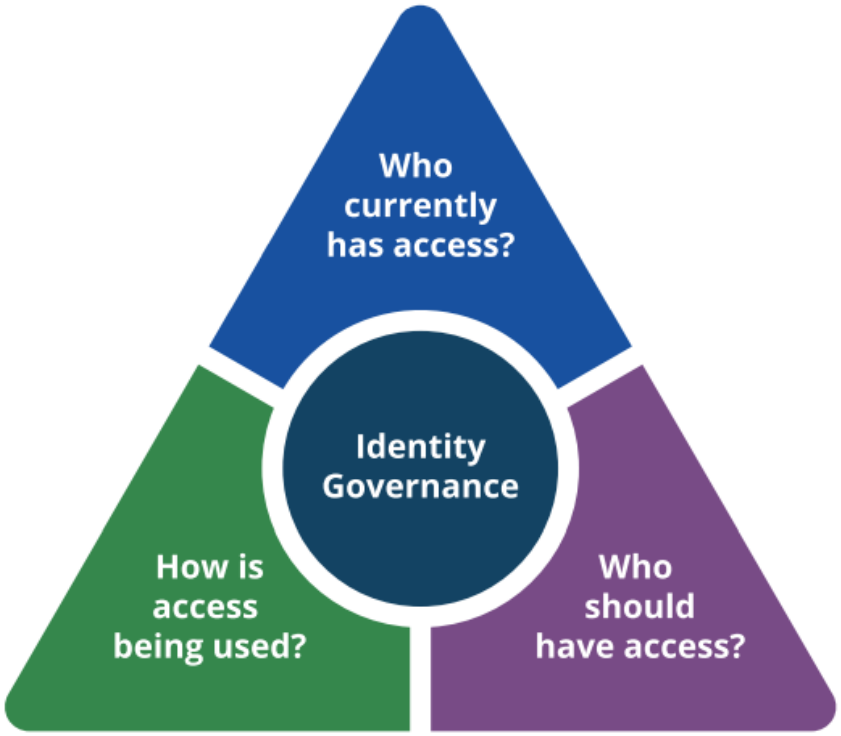

Рис. 1.3. Основні питання Identity Governance [1]

Сьогодні більшість організацій працюють із поєднанням хмарних, SaaS та локальних систем і програм. Послуги надаються кількома каналами та кількома постачальниками послуг. Управління контролем доступу, незалежно від того, як він надається кінцевому користувачеві, є компетенцією управління ідентифікацією. Контроль доступу користувачів вбудований у наші програми, системи та інфраструктуру. Кожна система встановлює політику контролю доступу для захисту своїх даних. Цей процес контролю доступу часто виглядає простим для тих, хто не знайомий з процесом керування ним (рис. 1.4) [1].

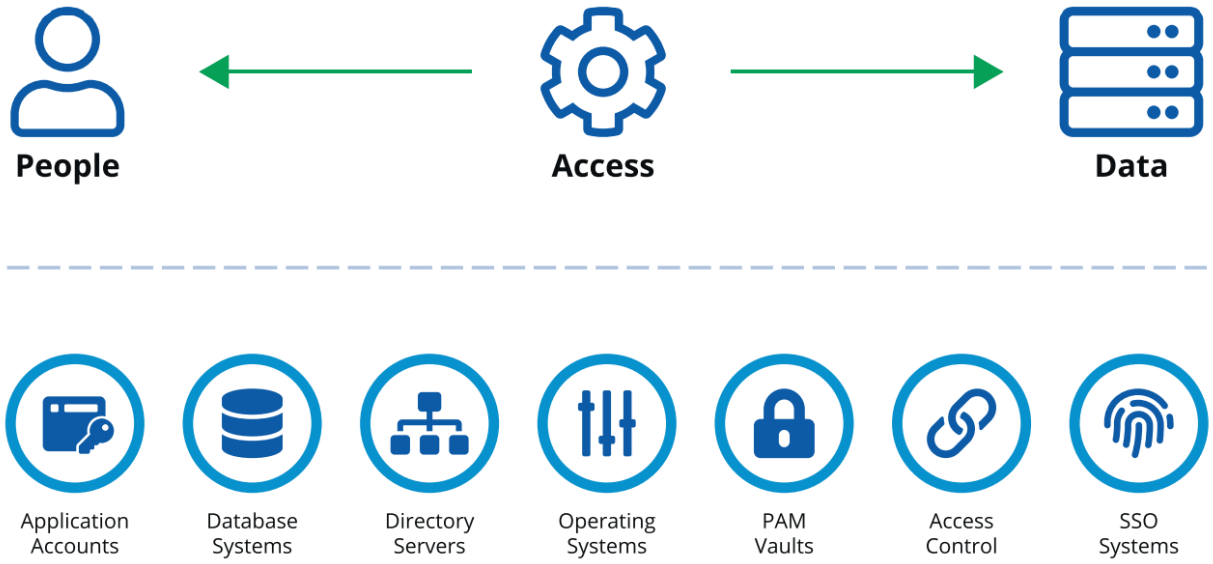

Рис. 1.4. Складність контролю доступу користувачів у корпоративних системах, що охоплюють вбудовані та зовнішні методи контролю [1]

Виявилося, що послідовне, всеосяжне та стійке управління цими різними формами контролю доступу вимагає спеціальної уваги. Навіть для найменшої організації реалізація контролю доступу в кінцевому підсумку вбудовується в облікові записи додатків, системи баз даних, каталоги, операційні системи та ряд зовнішніх рішень керування доступом, таких як єдиний вхід (SSO) і зовнішній контроль доступу на основі атрибутів. (ABAC) [1].

Рішення з керування ідентифікацією допомагають організації проводити інвентаризацію, аналізувати й розуміти, які права доступу надаються співробітникам, підрядникам і діловим партнерам у цих різних системах. Вони

забезпечують автоматизацію, контроль та керування всіма системами доступу, де б вони не знаходилися. Identity Governance забезпечує накладення високого рівня керування для ідентифікаторів, користувачів, облікових записів, привілеїв, прав і доступу, незалежно від того, як вони реалізовані [1].

Концепція контролю доступу на основі атрибутів (ABAC) існує вже багато років. Сутність цієї концепції полягає в контролі доступу, який включає списки контролю доступу, контроль доступу на основі ролей і метод ABAC для надання доступу на основі оцінки атрибутів [6].

Традиційно, контроль доступу базується на ідентифікації користувача, який запитує можливість виконання операції (наприклад, читання) над об’єктом (наприклад, файлом) або безпосередньо, або за допомогою попередньо визначених типів атрибутів, таких як ролі або групи. призначено цьому користувачеві [6].

Практики відзначають, що цей підхід до контролю доступу часто є громіздким у керуванні, оскільки необхідно пов’язувати можливості безпосередньо з користувачами або їхніми ролями чи групами. Також було відмічено, що кваліфікатори запитувача ідентичності, груп і ролей часто є недостатніми для вираження політик контролю доступу в реальному світі. Альтернативою є надання або відхилення запитів користувачів на основі довільних атрибутів користувача та довільних атрибутів об’єкта, а також умов середовища, які можуть бути загальновизнаними та більш відповідними відповідним політикам. Цей підхід часто називають ABAC [6].

ABAC – це логічна модель управління доступом, яку можна відрізнити, оскільки вона контролює доступ до об’єктів, оцінюючи правила щодо атрибутів сутностей (суб’єкт та об’єкт), операцій та середовища, що належать до запиту. Системи ABAC здатні забезпечувати дотримання концепції дискреційного контролю доступу (Discretionary Access Control, DAC), так і мандатного контролю доступу (Mandatory Access Control, MAC). ABAC забезпечує точне управління доступом, що дозволяє використовувати більшу кількість дискретних входів для ухвалення рішення про контроль доступу, забезпечуючи більший набір можливих

комбінацій цих змінних для відображення більшого та більш певного набору можливих правил для вираження політик [6].

Модель ABAC визначає доступ (тобто операції над системними об’єктами) шляхом зіставлення поточного значення атрибутів суб’єкта, атрибутів об’єкта та умов середовища з вимогами, зазначеними у правилах керування доступом.

Атрибути – це характеристики суб’єкта, об’єкта чи умов середовища. Атрибути містять інформацію, задану парою «ім’я-значення».

Суб’єкт – це людина-користувач або non-person entity (NPE), наприклад, пристрій, який видає запити доступу для виконання операцій з об’єктами. Суб’єктам надається один або кілька атрибутів. Для цілей цього документа передбачається, що суб’єкт та користувач є синонімами.

Об’єкт – це системний ресурс, доступ до якого керується системою ABAC, наприклад, пристрої, файли, записи, таблиці, процеси, програми, мережі або домени, що містять або отримують інформацію.

Це може бути ресурс або запитаний об'єкт, а також усе, над чим може бути виконана операція суб'єктом, включаючи дані, програми, служби, пристрої та мережі.

Операція – це виконання функції на запит суб’єкта над об’єктом. Операції включають читання, запис, редагування, видалення, копіювання, виконання та зміна.

Політика – це уявлення правил чи відносин, які дозволяють визначити, чи слід дозволити запитаний доступ, враховуючи значення атрибутів суб’єкта, об’єкта та, можливо, умов середовища.

Управління доступом на основі атрибутів (ABAC): метод управління доступом, при якому запити суб’єкта на виконання операцій з об’єктами надаються або відхиляються на основі призначених атрибутів суб’єкта, призначених атрибутів об’єкта, умов середовища та набору політик, які зазначені в умовах цих атрибутів та умов [6].

Умови середовища: операційний або ситуативний контекст, де виникають запити доступу. Умови середовища – це зумовлені характеристики середовища.

Характеристики середовища не залежать від суб'єкта або об'єкта і можуть включати поточний час, день тижня, місцезнаходження користувача або рівень загрози.

Визначення високорівнева модель ABAC зображено на рис. 1.5, де ACM ABAC отримує запит доступу суб'єкта, потім перевіряє атрибути суб'єкта та об'єкта на відповідність певній політиці. Потім ACM визначає, які операції суб'єкт може виконувати з об'єктом.

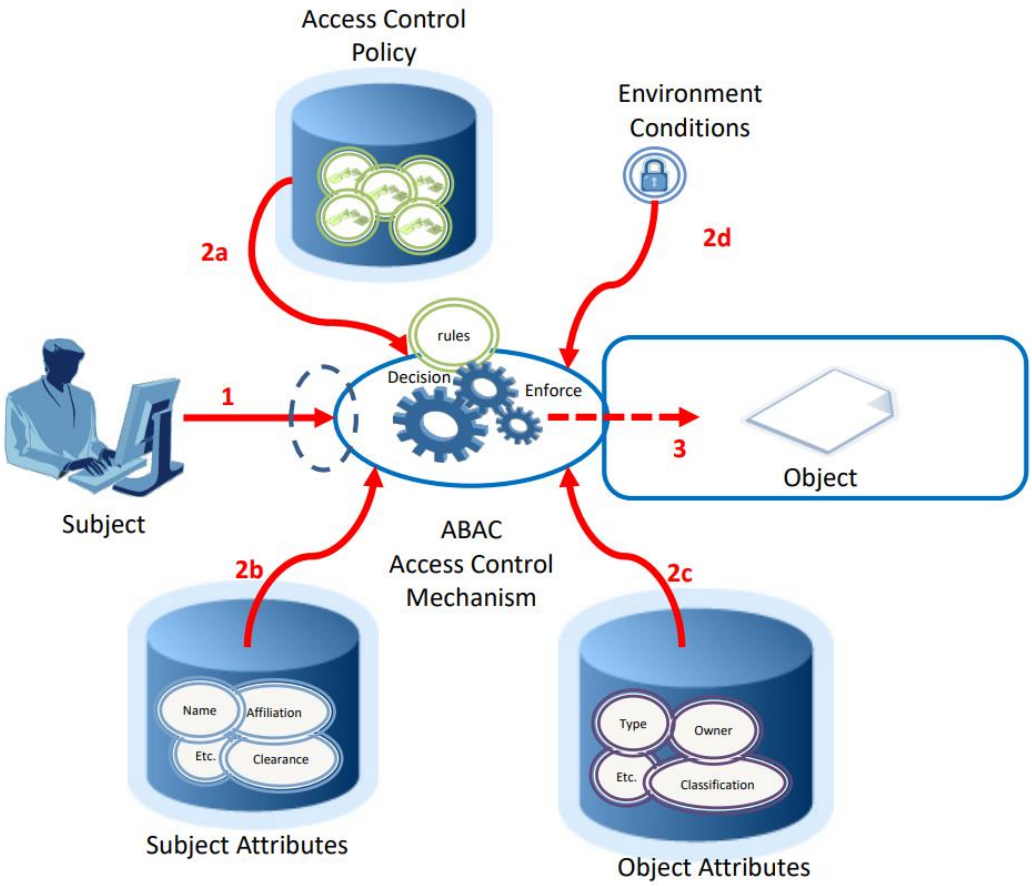

Рис. 1.5. Основні компоненти високорівневої моделі ABAC [6]

Позначки на рисунку: 1. суб'єкт запитує доступ до об'єкта; 2. механізм контролю доступу оцінює; a) правила, b) атрибути суб'єкта, c) атрибути об'єкта і d) умови середовища для обчислення рішення; 3. суб'єкту надається доступ до об'єкта, якщо він авторизований.

1.4. Аналіз існуючих рішень з управління доступом користувачів до хмарних сервісів та ресурсів

Розглянемо компоненти послуг ідентифікації, які показано на рис. 1.6.

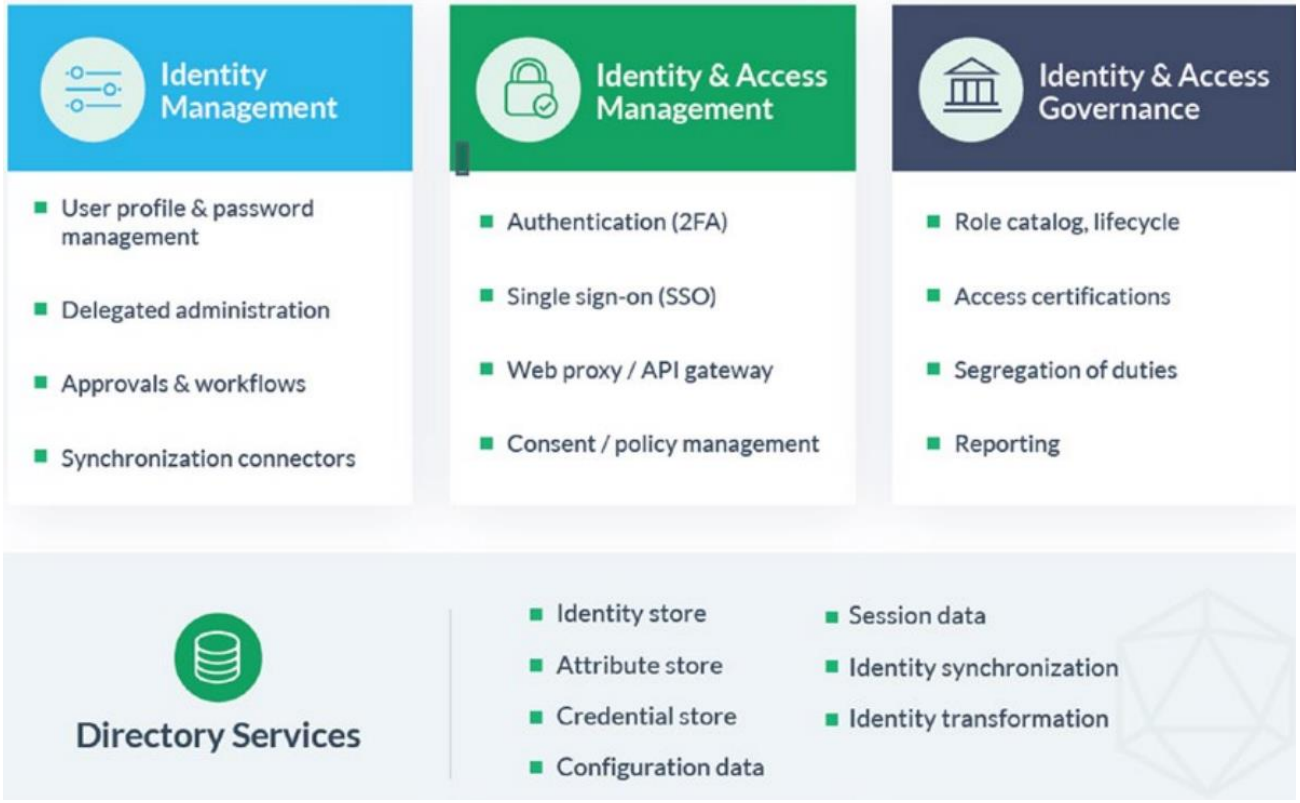

Рис. 1.6. Компоненти послуг ідентифікації [2]

Управління ідентифікацією. Цей термін іноді використовується для цілісного опису служби ідентифікації. Однак професіонали галузі мають на увазі лише одне, коли використовують термін IDM: управління синхронізацією систем за умов зміни інформації про людину. Події управління ідентифікацією відбуваються, коли запис про людину створюється, оновлюється чи видаляється.

Управління ідентифікацією та доступом є структурою політик і технологій, які гарантують, що потрібні користувачі мають відповідний доступ до технологічних ресурсів.

Identity and Access Governance (IAG) – це процес прийняття рішень і процес, за допомогою якого рішення впроваджуються (або не реалізуються). Управління ідентифікацією не є цілком технічним завданням. Це комбінація систем, правил і

процедур, які визначаються між окремою особою та організацією щодо прав, використання та захисту особистої інформації з метою автентифікації індивідуальних ідентичностей та надання дозволів та привілеїв у межах систем та підприємств або між ними [2].

Для впровадження якісної інфраструктури ідентифікації підприємства не можна ігнорувати важливість IDM. Якщо основні дані, які використовуються платформою IAM, неправильні, трапиться погане. Платформа IAM – це лише один споживач даних ідентифікації з системи IDM. Багато систем вимагають актуальних ідентифікаційних даних. Невиконання якісних процесів управління ідентифікацією призведе до проблем із безпекою та втрати продуктивності [2].

В [2] зазначається, що IDM і IAG – це не виключно технічні проблеми. Розгортання програмного забезпечення – це лише частина рішення. Існують бізнес-задачі, які також потрібно вирішити. Нерідкі випадки, коли проекти IDM та IAG вимагають значних витрат часу від кожного в організації. Швидкого рішення не існує, і всі рівні управління повинні бути залучені до розробки стратегії IDM.

Поведінку кінцевих користувачів, можливо, доведеться змінити – отже, IDM також є культурним. Впровадження систем IDM та IAG може вимагати значної кількості конфігурації та налаштування [2].

Багато організацій здійснюють цифрову трансформацію: все більше робочих навантажень виконується у програмах SaaS та хмарних платформах. Перехід до гібридної або повністю віддаленої робочої сили також прискорив доступ користувачів в обхід корпоративних мереж. Для керування цими змінами організації звертаються до постачальників IDaaS як основного постачальника посвідчень (IDP). У відповідь постачальники розширюють широту своїх можливостей IDaaS за рахунок придбання та органічної розробки, виходячи за рамки базових каталогів єдиного входу та базових каталогів, які лягли в основу більшості платформ IDaaS [10].

Внаслідок цієї тенденції IDaaS для корпоративних клієнтів має шукати постачальників, які демонструють [10]:

основні функції IDP всього спектра корпоративних ресурсів. Постачальники

IDaaS повинні надавати широку готову підтримку єдиного входу для корпоративних додатків (SaaS та локально) та корпоративних ресурсів, включаючи готові з'єднувачі для підключення нових додатків SaaS, додавання користувачів для SSO та надання/скасування доступу користувачів. Рішення IDaaS повинні відповідати встановленим стандартам ідентифікації, таким як SAML, Open ID Connect (OIDC), SCIM (Cross-domain Identity Management) та WS-Fed, та підтримувати інтеграцію єдиного входу для кінцевих точок Windows та Mac, мобільних пристроїв та пристроїв Інтернету речей (IoT). Їм також необхідно надати цільові інформаційні панелі та звіти, щоб допомогти оптимізувати поточні операції IDP. Каталог користувачів рішення IDaaS має бути здатним служити як основний каталог, який керує іншими каталогами та має підтримку делегованого адміністрування та застосування політик у доменах;

багатофакторна автентифікація (MFA) та включення без пароля. Постачальники IDaaS повинні мати стратегію, яка допомагає клієнтам відмовитися від пароля та перейти до більш простих у використанні, більш надійних методів автентифікації без пароля. Підтримка специфікацій FIDO2 (особливо WebAuthn) та партнерство зі спеціалізованими постачальниками без пароля – гарна відправна точка. Провідні постачальники IDaaS надають множину варіантів автентифікації (як власних, так і через партнерів), а також автентифікацію на основі ризиків та впорядкування робочого процесу, щоб вийти за межі однофакторної відсутності пароля та надати клієнтам найбезпечніший вибір з усіх – без пароля у поєднанні з MFA. Провідні постачальники також повинні мати ноу-хау та послуги для переведення клієнтів на шлях без пароля. Враховуючи можливе співіснування з паролями, що триває;

можливості розвитку для керування життєвим циклом користувачів та адаптації додатків. Постачальники IDaaS повинні розширювати можливості керування життєвим циклом користувачів, щоб забезпечити можливість застосування мінімальних прав доступу для всіх співробітників, тимчасових працівників та ділових партнерів. Має бути хороший базовий план для ініціалізації/деініціалізації від IDaaS та кожного з додатків. Постачальники

повинні мати встановлений та постійно зростаючий список попередньо створених з'єднувачів SCIM для більш швидкого та стандартизованого підходу до ініціалізації користувачів. Більш просунуті рішення пропонуватимуть робочі процеси запиту доступу та затвердження за допомогою візуальних інструментів з низьким рівнем коду або без коду для узгодження автоматизованих процесів із різними бізнес-політиками. Інші можливості, такі як контроль доступу на основі часу, інтеграція з системами продажу квитків служби підтримки, управління правами та аналітика ідентифікаційних даних також додають значну цінність.

На рис. 1.8 [10] показано оцінки Forrester Wave постачальників на ринку IDaaS для підприємств. Вони оцінювались за показниками числа запропонованих технологій, стратегій та представлень на ринку.

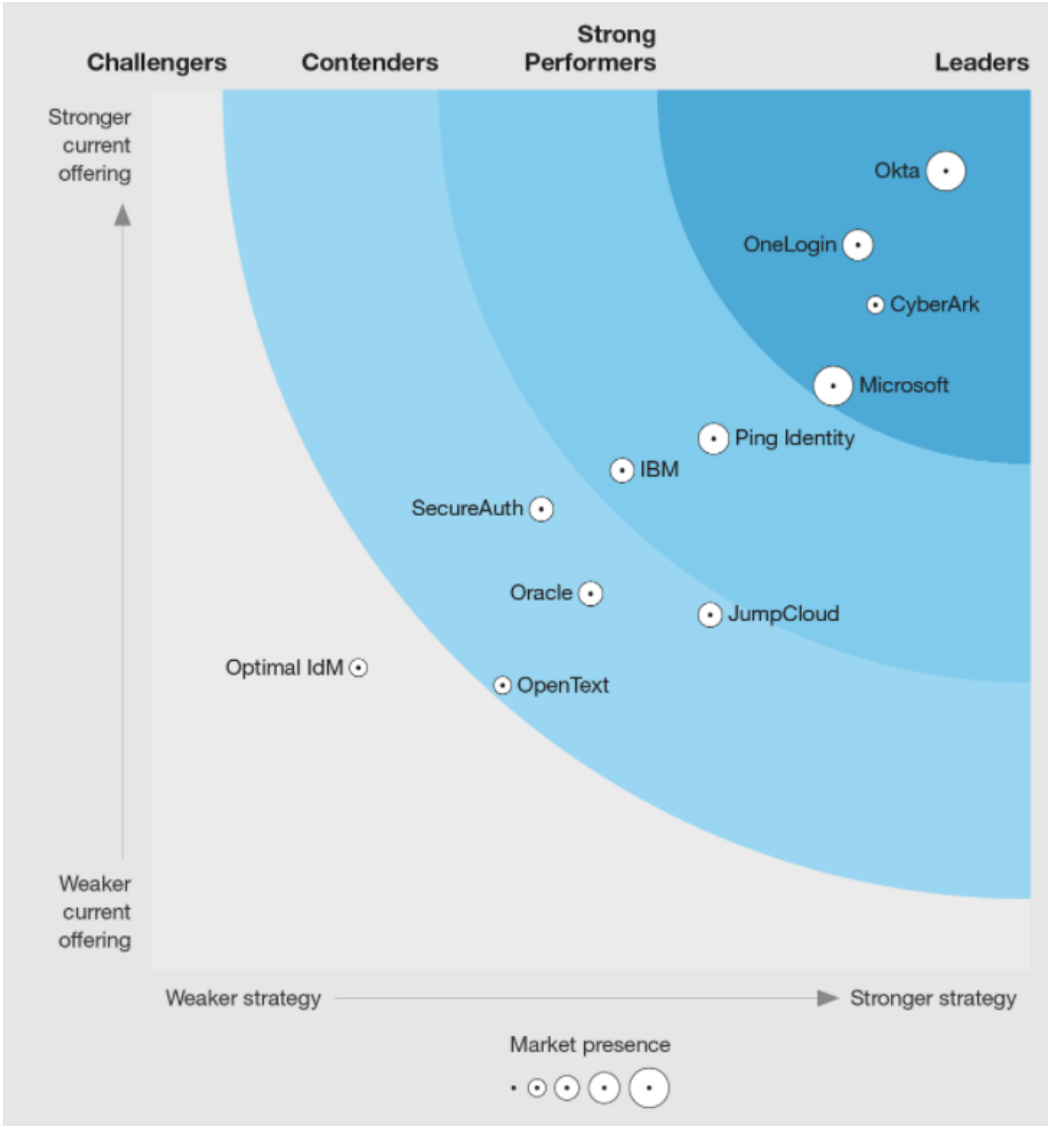

Рис. 1.7. Оцінка Forrester Wave провідних постачальників на ринку IDaaS для підприємств [10]

	Forrester's weighting	CyberArk	IBM	JumpCloud	Microsoft	Okta	OneLogin
Current offering	50%	3.78	2.84	2.02	3.32	4.54	4.12
Single sign-on	20%	3.00	3.00	3.00	5.00	5.00	5.00
User authentication	16%	5.00	3.00	1.00	3.00	5.00	5.00
User lifecycle management	12%	3.00	3.00	1.00	3.00	5.00	3.00
User directory	11%	3.00	3.00	3.00	3.00	3.00	5.00
Secure access	8%	5.00	1.00	0.00	5.00	5.00	3.00
User experience and navigation	12%	5.00	3.00	5.00	1.00	5.00	5.00
Reporting and compliance	12%	5.00	3.00	1.00	3.00	3.00	1.00
Performance and availability	9%	1.00	3.00	1.00	3.00	5.00	5.00
Strategy	50%	4.12	2.68	3.18	3.88	4.52	4.02
Product vision	25%	5.00	1.00	3.00	3.00	5.00	5.00
Innovation roadmap	20%	5.00	3.00	3.00	3.00	5.00	3.00
Market approach	10%	3.00	3.00	3.00	5.00	5.00	3.00
Execution roadmap	15%	3.00	3.00	3.00	5.00	3.00	5.00
Supporting products and services	11%	5.00	3.00	3.00	3.00	5.00	5.00
Commercial model	9%	3.00	5.00	5.00	5.00	3.00	3.00
Partner ecosystem	10%	3.00	3.00	3.00	5.00	5.00	3.00
Market presence	0%	1.80	2.60	2.10	5.00	5.00	3.40
Enterprise IDaaS revenue	70%	1.00	3.00	2.00	5.00	5.00	3.00
Enterprise IDaaS revenue growth	10%	5.00	3.00	5.00	5.00	5.00	3.00
Enterprise IDaaS installed base	20%	3.00	1.00	1.00	5.00	5.00	5.00

Рис. 1.8. Forrester Wave: IDaaS For Enterprise Scorecard, Q3 2021 [10]

Компанія Okta є лідером завдяки своїй всеосяжній незалежній платформі ідентифікації. Okta – найбільший постачальник IDaaS у чистому вигляді за доходами та кількістю клієнтів. Вендор завершив придбання постачальника CIAM Auth0 за 6,5 млрд доларів станом на травень 2021 року. Okta планує: 1) удосконалити управління доступом із розширеним делегуванням користувачів, можливостями самообслуговування та сигналами для прийняття рішень про доступ; 2) удосконалити керування життєвим циклом користувачів за рахунок

можливостей керування ідентифікацією; та 3) адресу безпечного доступу для привілейованих користувачів [10].

Платформа Okta IDaaS має велику глибину і широту встановлених конекторів з більш ніж 7000 для SSO (1600 SAML, 65 OIDC) і більше 200 для ініціалізації та деініціалізації користувачів (SCIM). Okta підтримує параметри без пароля, включаючи WebAuthn, та забезпечує рівні автентифікації, узгоджені з NIST. Рішення пропонує привабливий інтерфейс користувача з самообслуговуванням затвердження запитів на доступ для користувачів і підходами без коду/з низьким кодом, такими як Okta Workflows. Звітність є надійною, настроюваною та дієвою [10].

Інтеграція з успадкованими локальними системами додатків через Access Gateway є більш новою та менш розвиненою, ніж деякі інші рішення. Okta найкраще підходить для організацій, у яких більша частина робочих навантажень знаходиться в SaaS або в хмарі (хоча локальні веб-додатки підтримуються через Access Gateway) і яким потрібний надійний, незалежний повнофункціональний IDP на основі IDaaS. Інтеграція з успадкованими локальними системами додатків через Access Gateway є більш новою та менш розвиненою, ніж деякі інші рішення. Okta найкраще підходить для організацій, у яких багато робочих навантажень виконуються в SaaS або у хмарі (хоча локальні веб-додатки підтримуються через Access Gateway) і яким потрібний надійний, незалежний, повнофункціональний IDP на основі IDaaS [10].

Інтеграція з успадкованими локальними системами додатків через Access Gateway є більш новою та менш розвиненою, ніж деякі інші рішення. Okta найкраще підходить для організацій, у яких багато робочих навантажень виконуються в SaaS або в хмарі (хоча локальні веб-додатки підтримуються через Access Gateway) і яким потрібний надійний, незалежний, повнофункціональний IDP на основі IDaaS [10].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ХМАРНИХ СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES

2.1. Дослідження можливостей використання хмарних сервісів та ресурсів Amazon Web Services

Amazon Web Services (AWS) – це найпоширеніша у світі хмарна платформа з найширшими можливостями, що надає понад 200 повнофункціональних сервісів для центрів обробки даних по всій планеті. Мільйони клієнтів, у тому числі стартапи, які стали лідерами за швидкістю зростання, найбільші корпорації та передові урядові установи, використовують AWS для зниження витрат, підвищення гнучкості та прискореного впровадження інновацій [7].

Amazon Web Services (AWS) – це платформа веб-сервісів, яка пропонує рішення для обчислень, зберігання та роботи в мережі на різних рівнях абстракції. Наприклад, ви можете використовувати сховище на рівні блоків (низький рівень абстракції) або сильно розподілене сховище об’єктів (високий рівень абстракції) для зберігання ваших даних [3].

Ви можете використовувати ці служби для розміщення веб-сайтів, запуску корпоративних програм і копіювання величезних обсягів даних. Веб-сервіси доступні через Інтернет за допомогою типових протоколів веб-програм (наприклад, HTTP) і використовуються машинами або людьми через інтерфейс користувача [3].

Найвідоміші послуги, що надаються AWS, – це EC2, який пропонує віртуальні машини, і S3, який пропонує ємність для зберігання даних. Сервіси в AWS добре працюють разом та їх можна використовувати, щоб відтворити наявні налаштування локальної мережі, або для створення нового налаштування з нуля. Модель ціноутворення на послуги – оплата за використання [3].

Визначення Національного інституту стандартів і технологій: *хмарні*

обчислення – це модель для забезпечення повсюдного, зручного мережевого доступу на вимогу до спільного пулу налаштовуваних обчислювальних ресурсів (мереж, віртуальних машин, сховища, програм і служб), які можна швидко надати та випустити з мінімальними зусиллями керівництва або взаємодії з постачальником послуг [3].

AWS – це загальнодоступна хмара. Служби хмарних обчислень також мають кілька класифікацій [3]:

Інфраструктура як послуга (IaaS) – пропонує фундаментальні ресурси, такі як можливості обчислення, зберігання та роботи в мережі, використовуючи віртуальні машини, такі як Amazon EC2, Google Compute Engine та Microsoft Azure.

Платформа як послуга (PaaS) – надає платформи для розгортання спеціальних програм у хмарі, таких як AWS Elastic Beanstalk, Google App Engine і Heroku.

Програмне забезпечення як послуга (SaaS) – поєднує інфраструктуру та програмне забезпечення, що працює в хмарі, включаючи офісні програми, такі як Amazon WorkSpaces, Google Apps for Work і Microsoft Office 365. Портфель продуктів AWS містить IaaS, PaaS і SaaS.

Інноваційні бізнес-додатки з такою ж масштабованістю на вимогу, надійністю, ціноутворенням з оплатою по мірі використання та машинним навчанням, які керують хмарною інфраструктурою AWS [11].

AWS має значно більше послуг і більше функцій у цих сервісах, ніж будь-який інший хмарний постачальник – від інфраструктурних технологій, таких як обчислення, зберігання та бази даних, до нових технологій, таких як машинне навчання та штучний інтелект, озера даних та аналітика та Інтернет речей. Це робить перенесення наявних додатків у хмару та створення майже всього, що ви можете собі уявити, швидше, простіше та дешевше (рис. 2.1).

AWS також має найглибшу функціональність у цих сервісах. Наприклад, AWS пропонує найширший вибір баз даних, спеціально створених для різних типів додатків, щоб ви могли вибрати правильний інструмент для роботи, щоб

отримати найкращу вартість та продуктивність.

Категорія	Опис послуги	Сервіс AWS
Лінія бізнес-додатків	Простий у використанні багатоканальний хмарний контакт-центр	Amazon Connect
	Багатоканальні маркетингові комунікації	Amazon Pinpoint
Програми для підвищення продуктивності	Створюйте програми для керування роботою вашої команди без кодування	Amazon Honeycode
	Зустрічі без розчарувань, відеодзвінки та чат	Amazon Chime
	Безпечне зберігання та обмін корпоративними документами	Amazon WorkDocs
	Безпечна електронна пошта та календар	Amazon WorkMail
	Розширте можливості своєї організації за допомогою Alexa	Alexa для бізнесу
Послуги розробника комунікацій	Обмін повідомленнями в режимі реального часу, аудіо, відео та показ екрана	Amazon Chime SDK
	Масштабна вхідна та вихідна електронна пошта	Amazon Simple Email Service (SES)
	Гнучкі мобільні SMS та push-повідомлення	API Amazon Pinpoint
	Економічний SIP-транкінг і розширені функції телефонії	Голосовий роз'єм Amazon Chime
	Безпечна спільна робота та керування файлами	Amazon WorkDocs SDK

Рис. 2.1. Служби бізнес-додатків AWS [11]

AWS має найбільшу та найдинамічнішу спільноту з мільйонами активних клієнтів і десятками тисяч партнерів по всьому світу. Клієнти практично в кожній галузі та будь-якого розміру, включаючи стартапи, підприємства та організації державного сектору, використовують усі можливі варіанти використання AWS. Партнерська мережа AWS (APN) включає тисячі системних інтеграторів, які спеціалізуються на послугах AWS, і десятки тисяч незалежних постачальників програмного забезпечення (ISV), які адаптують свою технологію для роботи на AWS [11].

AWS створена як найбільш гнучка та безпечна середа хмарних обчислень, доступна сьогодні. Наша основна інфраструктура створена, щоб задовольнити вимоги безпеки для військових, глобальних банків та інших високочутливих організацій. Це підкріплено широким набором інструментів хмарної безпеки з 230

службами та функціями безпеки, відповідності та управління. AWS підтримує 90 стандартів безпеки та сертифікатів відповідності, а всі 117 служб AWS, які зберігають дані клієнтів, пропонують можливість шифрувати ці дані [11].

2.2. Призначення, можливості та функції управління доступом користувачів до хмарних сервісів та ресурсів AWS IAM

AWS Identity and Access Management (IAM) – це веб-сервіс, який допомагає безпечно контролювати доступ до ресурсів AWS. IAM використовується, щоб контролювати, хто автентифікований (ввійшов) і авторизований (має дозволи) на використання ресурсів. Коли вперше створюється обліковий запис AWS, ви починаєте з єдиного входу, який має повний доступ до всіх служб і ресурсів AWS в обліковому записі. Ця особа називається root-користувачем облікового запису AWS, і доступ до нього здійснюється шляхом входу за допомогою адреси електронної пошти та пароля, які ви використовували для створення облікового запису. Наполегливо рекомендується не використовувати користувача root для своїх повсякденних завдань, навіть адміністративних. Натомість необхідно дотримуватися найкращих методів використання лише користувача root для створення першого користувача IAM. Потім надійно заблокуйте облікові дані користувача root і використовуйте їх для виконання лише кількох завдань керування обліковими записами та службами [12].

AWS IAM забезпечує точний контроль доступу у всіх сервісах AWS. За допомогою IAM ви можете вказати, хто може отримувати доступ до певних сервісів та ресурсів та за яких умов. Завдяки політикам IAM ви керуєте дозволами для співробітників та систем, надаючи дозволи з найменшими привілеями.

Розглянемо приклади використання AWS IAM. Загальний принцип роботи AWS IAM показано на рис. 2.2. За допомогою IAM можна керувати дозволами AWS для співробітників та робочих навантажень. Для співробітників рекомендується використовувати AWS Single Sign-On (AWS SSO), щоб керувати доступом до облікових записів AWS та дозволами в межах облікових записів. З

AWS SSO можна легко призначати ролі та політики IAM і керувати ними в масштабах всієї організації. Для робочих навантажень використовуються ролі та політики IAM та надаються лише необхідні дозволи.

Рис. 2.2. Загальний принцип роботи AWS IAM [12]

Здійснюється точний контроль доступу. Використовуючи політики IAM, надається доступ до певних API сервісів та ресурсів AWS. Ви також можете визначити конкретні умови для надання доступу, наприклад, певна організація AWS або використання певного сервісу AWS.

Встановлюються обмеження дозволів та периметри даних у всій організації AWS. Завдяки AWS Organizations можна використовувати політики керування сервісами (SCP) для встановлення обмежень дозволів, яким будуть відповідати всі користувачі та ролі IAM в облікових записах організації. Незалежно від того, чи починаєте ви працювати з SCP або вони вже є, можна використовувати консультанта з доступу IAM для того, щоб впевнено обмежувати дозволи.

Створюються дозволи з мінімальними привілеями завдяки IAM Access Analyzer. Досягнення принципу мінімальних привілеїв – це безперервний цикл видачі відповідних точних дозволів у міру появи вимог. IAM Access Analyzer допомагає оптимізувати налаштування, перевірку та уточнення дозволів.

Здійснюється автоматичне масштабування точних дозволів за допомогою ABAC. Управління доступом на основі атрибутів (ABAC) – це стратегія

авторизації для створення деталізованих дозволів на базі атрибутів користувача, таких як відділ, робоча роль і назва команди. За допомогою ABAC можна скоротити кількість дозволів, необхідних для точного керування обліковим записом AWS.

Завдяки точним дозволам IAM можна визначати, хто отримує доступ. Потім IAM застосовує ці дозволи до кожного запиту. За замовчанням доступ заборонено та можливий лише в тому випадку, коли вибрано значення «Дозволено».

Розглянемо функції IAM. IAM надає такі функції [12]:

Спільний доступ до облікового запису AWS. Ви можете надати іншим людям дозвіл на адміністрування та використання ресурсів у вашому обліковому записі AWS, не повідомляючи свій пароль або ключ доступу.

Детальні дозволи. Ви можете надавати різні дозволи різним людям для різних ресурсів. Наприклад, ви можете надати деяким користувачам повний доступ до Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift та інших служб AWS. Для інших користувачів ви можете надати доступ лише для читання лише до деяких сегментів S3 або дозволити адмініструвати лише деякі екземпляри EC2 або отримати доступ до вашої платіжної інформації, але нічого іншого.

Безпечний доступ до ресурсів AWS для програм, які працюють на Amazon EC2. Ви можете використовувати функції IAM для безпечного надання облікових даних для програм, які працюють на екземплярах EC2. Ці облікові дані надають вашій програмі дозволи на доступ до інших ресурсів AWS. Приклади включають сегменти S3 і таблиці DynamoDB.

Багатофакторна автентифікація (MFA). Ви можете додати двофакторну автентифікацію до свого облікового запису та окремих користувачів для додаткової безпеки. З MFA ви або ваші користувачі повинні надати не тільки пароль або ключ доступу для роботи зі своїм обліковим записом, а й код зі спеціально налаштованого пристрою.

Об'єднання ідентифікації. Ви можете дозволити користувачам, які вже мають паролі в інших місцях, наприклад, у вашій корпоративній мережі або у

постачальника ідентифікаційних даних в Інтернеті, отримати тимчасовий доступ до вашого облікового запису AWS.

Ідентифікаційна інформація для гарантії. Якщо ви використовуєте AWS CloudTrail, ви отримуєте записи журналу, які містять інформацію про тих, хто зробив запити на ресурси у вашому обліковому записі. Ця інформація заснована на ідентифікаторах IAM.

Відповідність стандарту PCI DSS. IAM підтримує обробку, зберігання та передачу даних кредитних карток продавцем або постачальником послуг, і його було підтверджено як відповідність вимогам Payment Card Industry (PCI) Data Security Standard (DSS).

Інтеграція з багатьма сервісами AWS.

Узгодження IAM, як і багато інших служб AWS, є узгодженим. IAM досягає високої доступності шляхом реплікації даних на кількох серверах у центрах обробки даних Amazon по всьому світу. Якщо запит на зміну деяких даних успішний, зміна фіксується та безпечно зберігається. Однак зміна має бути відтворена в IAM, що може зайняти деякий час. Такі зміни включають створення або оновлення користувачів, груп, ролей або політик. Ми рекомендуємо не включати такі зміни IAM у критичні шляхи коду високої доступності вашої програми. Замість цього внесіть зміни в IAM в окремій підпрограмі ініціалізації або налаштування, яку ви запускаєте рідше. Також переконайтеся, що зміни були поширені до того, як робочі процеси залежать від них.

Безкоштовне використання. AWS IAM і AWS Security Token Service (AWS STS) – це функції вашого облікового запису AWS, які пропонуються без додаткової плати. З вас стягується плата, лише якщо ви отримуєте доступ до інших служб AWS за допомогою своїх користувачів IAM або тимчасових облікових даних безпеки AWS STS.

Розглянемо, як працює AWS IAM. Перш ніж створювати користувачів, ви повинні зрозуміти, як працює IAM. IAM забезпечує інфраструктуру, необхідну для контролю автентифікації та авторизації для вашого облікового запису. Інфраструктура IAM включає такі елементи (рис. 2.3): умови, принципал, запит,

автентифікація, авторизація, дії або операції, ресурси [12].

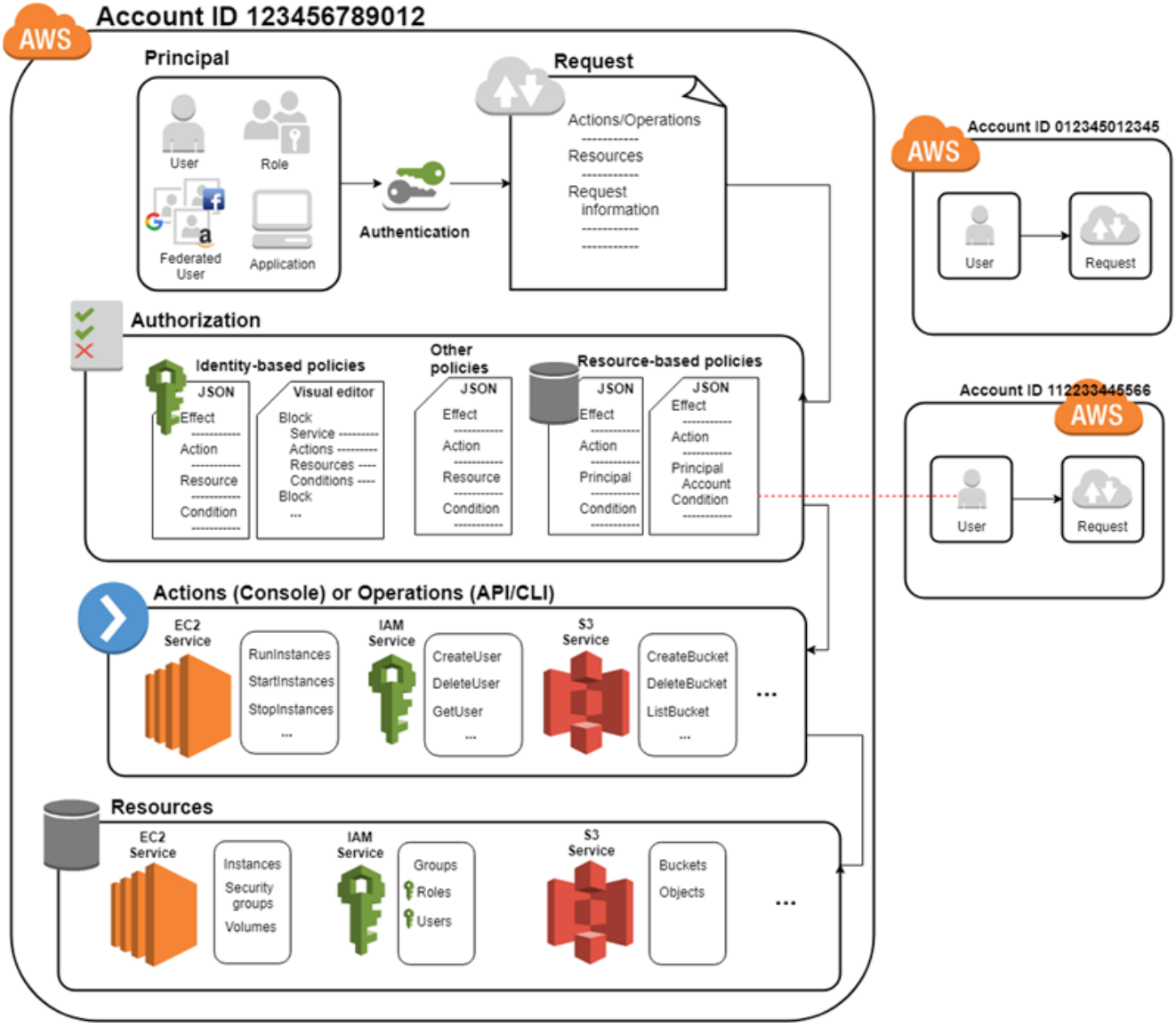

Рис. 2.3. Складові частини системи AWS IAM [12]

Ресурси IAM: об’єкти користувача, групи, ролі, політики та постачальники ідентифікаційних даних, які зберігаються в IAM. Як і в інших сервісах AWS, ви можете додавати, редагувати та видаляти ресурси з IAM.

Ідентифікації IAM:

Об’єкти ресурсів IAM, які використовуються для ідентифікації та групування. Ви можете прикріпити політику до ідентифікатора IAM. До них належать користувачі, групи та ролі.

Суб’єкти IAM – об’єкти ресурсу IAM, які AWS використовує для

автентифікації. До них належать користувачі та ролі IAM.

Принципал – особа або програма, яка використовує root-користувача облікового запису AWS, користувача IAM або роль IAM для входу та надсилання запитів до AWS. До принципалів належать об’єднані користувачі та передані ролі.

Принципал – головним є людина або додаток, яка може зробити запит на дії або операції по ресурсу AWS. Принципал автентифікується як кореневий користувач облікового запису AWS або сутність IAM для надсилання запитів до AWS. Як найкраща практика, не використовуйте облікові дані користувача root для щоденної роботи. Замість цього створюйте сутності IAM (користувачів і ролей). Ви також можете підтримувати федеративних користувачів або програмний доступ, щоб дозволити програмі отримати доступ до вашого облікового запису AWS.

Запит: коли принципал намагається використати Консоль керування AWS, API AWS або AWS CLI, цей принципал надсилає запит до AWS. Запит містить таку інформацію [12]:

дії або операції – дії або операції, які хоче виконати принципал. Це може бути дія в Консолі керування AWS або операція в AWS CLI або AWS API;

ресурси – об’єкт ресурсу AWS, на якому виконуються дії або операції;

принципал – особа або програма, яка використовувала об’єкт (користувача чи роль) для відправлення запиту. Інформація про принципала включає політики, пов’язані з сутністю, яку принципал використовував для входу;

дані середовища – інформація про IP-адресу, агент користувача, статус увімкненого SSL або час доби;

дані ресурсу – дані, пов’язані з ресурсом, який запитується. Це може включати таку інформацію, як ім’я таблиці DynamoDB або тег на екземплярі Amazon EC2.

AWS збирає інформацію запиту в контекст запиту , який використовується для оцінки та авторизації запиту.

Автентифікація. Щоб надіслати запит до AWS, принципал має пройти автентифікацію (ввійти в AWS), використовуючи свої облікові дані. Деякі сервіси,

такі як Amazon S3 і AWS STS, допускають кілька запитів від анонімних користувачів. Однак вони є винятком із правил.

Щоб пройти автентифікацію з консолі як користувач root, ви повинні увійти, використовуючи свою адресу електронної пошти та пароль. Як користувач IAM, вкажіть ідентифікатор або псевдонім свого облікового запису, а потім ім’я користувача та пароль. Щоб пройти автентифікацію за допомогою API або AWS CLI, потрібно надати ключ доступу та секретний ключ. Від вас також може знадобитися надати додаткову інформацію безпеки. Наприклад, AWS рекомендує використовувати багатофакторну автентифікацію (MFA), щоб підвищити безпеку вашого облікового запису.

Авторизація: ви також повинні бути авторизовані (дозволені) для виконання вашого запиту. Під час авторизації AWS використовує значення з контексту запиту для перевірки правил, які застосовуються до запиту. Потім він використовує політику, щоб визначити, дозволити чи відхилити запит. Більшість політик зберігаються в AWS як документи JSON і вказують дозволи для основних сутностей. Існує кілька типів полісів, що може вплинути на те, чи буде запит авторизований. Щоб надати своїм користувачам дозволи на доступ до ресурсів AWS у власному обліковому записі, вам потрібні лише політики на основі ідентифікації. Політики на основі ресурсів популярні для надання доступу між обліковими записами. Інші типи політики є розширеними функціями, і їх слід використовувати обережно.

AWS перевіряє кожну політику, яка застосовується до контексту вашого запиту. Якщо одна політика дозволів містить заборонену дію, AWS відхиляє весь запит і припиняє оцінку. Це називається явним запереченням . Оскільки запити відхиляються за замовчуванням, AWS авторизує ваш запит, лише якщо кожна частина вашого запиту дозволена відповідною політикою дозволів. Логіка оцінки запиту в межах одного облікового запису відповідає таким загальним правилам:

За замовчуванням усі запити відхиляються. (Загалом, запити, зроблені з використанням облікових даних root користувача облікового запису AWS для ресурсів облікового запису, завжди дозволені).

Явний дозвіл у будь-якій політиці дозволів (на основі ідентифікаційних даних чи ресурсів) замінює це за замовчуванням.

Існування організації SCP, межі дозволів IAM або політика сеансу перевизначає дозвіл. Якщо існує один або кілька з цих типів політики, усі вони повинні дозволяти запит. В іншому випадку це неявно заперечується. Явна заборона в будь-якій політиці перевизначає будь-які дозволи.

Дії або операції. Після автентифікації та авторизації вашого запиту AWS схвалює дії або операції у вашому запиті. Операції визначаються службою і включають те, що ви можете робити з ресурсом, наприклад перегляд, створення, редагування та видалення цього ресурсу. Наприклад, IAM підтримує приблизно 40 дій для ресурсу користувача, включаючи такі дії: *CreateUser, DeleteUser, GetUser, UpdateUser.*

Ресурси. Після того, як AWS схвалить операції у вашому запиті, їх можна буде виконувати на відповідних ресурсах у вашому обліковому записі. Ресурс – це об’єкт, який існує в службі. Приклади включають екземпляр Amazon EC2, користувача IAM і сегмент Amazon S3. Сервіс визначає набір дій, які можна виконати з кожним ресурсом. Якщо ви створюєте запит на виконання непов’язаної дії з ресурсом, цей запит відхиляється. Наприклад, якщо ви надсилаєте запит на видалення ролі IAM, але надаєте ресурс групи IAM, запит не виконується.

2.3. Сутність моделі управління доступом користувачів на основі атрибутів в AWS IAM

Контроль доступу на основі атрибутів (ABAC) – це стратегія авторизації, яка визначає дозволи на основі атрибутів. У AWS ці атрибути називаються тегами. Ви можете прикріплювати теги до ресурсів IAM, зокрема до сутностей IAM (користувачів або ролей), а також до ресурсів AWS. Ви можете створити одну політику ABAC або невеликий набір політик для своїх керівників IAM. Ці політики ABAC можуть бути розроблені для того, щоб дозволити операції, коли

тег принципала збігається з тегом ресурсу. ABAC корисний у середовищах, які швидко розвиваються, і допомагає у ситуаціях, коли управління політикою стає громіздким [12].

Наприклад, ви можете створити три ролі за допомогою *access-project* ключа тегу. Встановіть значення тегу першої ролі на *Heart*, другої на *Sun*, а третьої на *Lightning* (рис. 2.4). Потім можна використовувати єдину політику, яка надає доступ, якщо роль і ресурс позначено однаковими тегами для *access-project* [12].

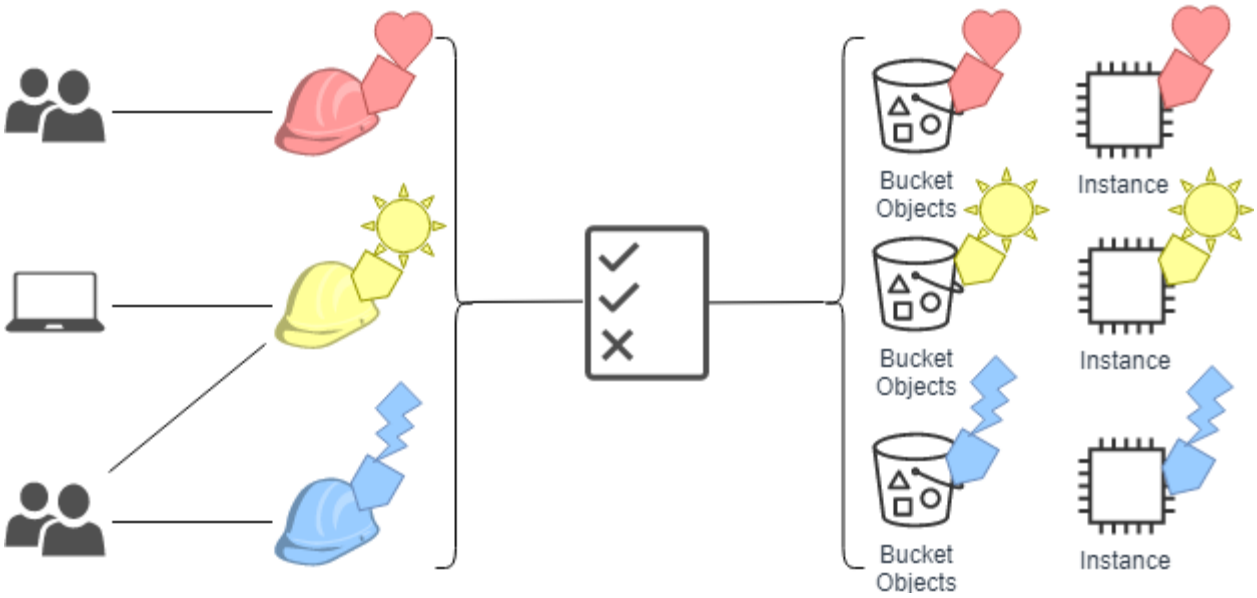

Рис. 2.4. Принцип контролю доступу на основі атрибутів (ABAC) [12]

Порівняння ABAC з традиційною моделлю RBAC [12].

Традиційна модель авторизації, що використовується в IAM, називається керуванням доступом на основі ролей (RBAC). RBAC визначає дозволи на основі службової функції людини, відомої за межами AWS як роль. У AWS роль зазвичай відноситься до ролі IAM, яка є особистістю в IAM, яку ви можете прийняти. IAM містить керовані політики для робочих функцій, які узгоджують дозволи з робочою функцією в моделі RBAC.

У IAM ви реалізуєте RBAC, створюючи різні політики для різних робочих функцій. Потім ви приєднуєте політики до ідентифікаційних даних (користувачів IAM, груп користувачів або ролей IAM). Як найкраща практика, ви надаєте мінімальні дозволи, необхідні для роботи функції. Це відомо як надання найменших привілеїв. Зробіть це, перерахувавши конкретні ресурси, до яких

може отримати доступ службова функція. Недоліком використання традиційної моделі RBAC є те, що коли співробітники додають нові ресурси, ви повинні оновлювати політики, щоб дозволити доступ до цих ресурсів.

Наприклад, припустимо, що у вас є три проекти з іменами *Heart*, *Sun*, і *Lightning*, над якими працюють ваші співробітники. Ви створюєте роль IAM для кожного проекту. Потім ви додаєте політику до кожної ролі IAM, щоб визначити ресурси, до яких може отримати доступ будь-хто, кому дозволено взяти на себе роль. Якщо працівник змінює роботу у вашій компанії, ви призначаєте йому іншу роль IAM. Людей або програм можна призначити на кілька ролей. Однак, *Sun* для проекту можуть знадобитися додаткові ресурси, наприклад, новий сегмент Amazon S3. У цьому випадку ви повинні оновити політику, додану до *Sun* ролі, щоб вказати новий ресурс сегмента. В іншому випадку *Sun* учасники проекту не матимуть доступу до нового сегмента (рис. 2.5).

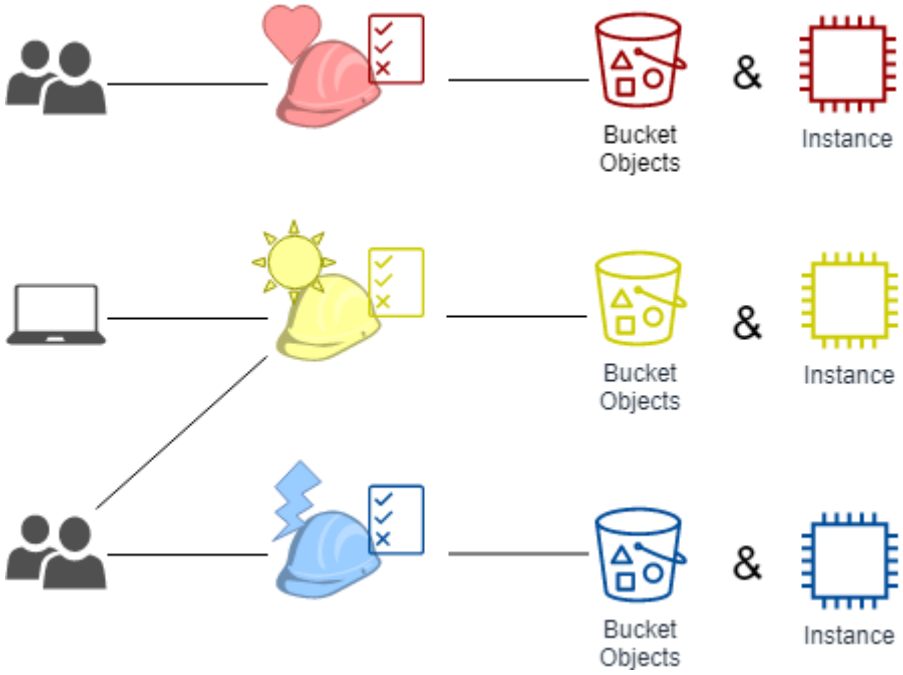

Рис. 2.5. Принцип керуванням доступом на основі ролей (RBAC) [12]

ABAC забезпечує наступні переваги перед традиційною моделлю RBAC [12]:

Інноваційне масштабування дозволів ABAC. Адміністратору більше не потрібно оновлювати існуючі політики, щоб дозволити доступ до нових ресурсів.

Наприклад, припустимо, що ви розробили свою стратегію ABAC за допомогою *access-project* тегу. Розробник використовує роль з тегом *access-project = Heart*. Коли учасникам *Heart* проекту потрібні додаткові ресурси Amazon EC2, розробник може створити нові екземпляри Amazon EC2 за допомогою тег *access-project = Heart*. Тоді будь-хто в *Heart* проекті може запускати та зупиняти ці екземпляри, оскільки їхні значення тегу збігаються.

ABAC вимагає менше політик. Оскільки вам не потрібно створювати різні політики для різних робочих функцій, ви створюєте менше політик. Цими політиками легше керувати.

Використовуючи ABAC, команди можуть швидко змінюватися та розвиватися. Це тому, що дозволи для нових ресурсів надаються автоматично на основі атрибутів. Наприклад, якщо ваша компанія вже підтримує проекти *Heart* та з *Sun* використанням ABAC, можна легко додати новий *Lightning* проект. Адміністратор IAM створює нову роль з тег *access-project = Lightning*. Для підтримки нового проекту змінювати політику не потрібно. Будь-хто, хто має дозвіл на виконання ролі, може створювати та переглядати екземпляри з тегом *access-project = Lightning*. Крім того, член команди може перейти від *Heart* проекту до *Lightning* проекту. Адміністратор IAM призначає користувача іншу роль IAM. Змінювати політику дозволів не потрібно.

Детальні дозволи можливі за допомогою ABAC. Коли ви створюєте політики, найкраще надавати найменші привілеї. Використовуючи традиційний RBAC, ви повинні написати політику, яка надає доступ лише до певних ресурсів. Однак, коли ви використовуєте ABAC, ви можете дозволити дії з усіма ресурсами, але лише якщо тег ресурсу збігається з тегом принципала.

Використовуйте атрибути співробітників зі свого корпоративного каталогу за допомогою ABAC. Ви можете налаштувати свого постачальника ідентифікаторів на основі SAML або веб-посвідчення на передачу тегів сеансу в AWS. Коли ваші співробітники об’єднуються в AWS, їхні атрибути застосовуються до їх результуючого принципала в AWS. Потім ви можете використовувати ABAC, щоб дозволити або відхилити дозволи на основі цих

атрибутів.

2.4. Призначення, можливості та функції централізованого управління доступом до облікових записів та додатків AWS Single Sign-On

IAM призначено для керування дозволами AWS для співробітників та робочих навантажень. Для співробітників рекомендується використовувати AWS Single Sign-On (AWS SSO), щоб керувати доступом до облікових записів AWS та дозволами в межах облікових записів. З AWS SSO можна легко призначати ролі та політики IAM і керувати ними в масштабах всієї організації. Для робочих навантажень використовуються ролі та політики IAM та видаються лише необхідні дозволи [13].

Сервіс AWS Single Sign-On (SSO) дозволяє централізовано керувати доступом до багатьох облікових записів AWS та бізнес-додатків. Також цей сервіс забезпечує користувачам доступ з єдиним входом до всіх закріплених за ними акаунтів та додатків. AWS SSO спрощує централізоване керування доступом та дозволами користувачів для всіх облікових записів в AWS Organizations. SSO налаштовує та обслуговує всі необхідні дозволи для облікових записів автоматично без додаткового налаштування окремих облікових записів. Користувальницькі дозволи можна задавати на основі загальних посадових обов’язків, а потім додатково налаштовувати відповідно до конкретних вимог безпеки. AWS SSO забезпечує також вбудовану підтримку інтеграції з багатьма бізнес-додатками (наприклад, Salesforce, Box та Microsoft 365) [13].

На порталі AWS SSO створюються посвідчення користувача та керувати ними, а також легко підключатися до вже існуючих джерел посвідчень, наприклад Microsoft Active Directory, Okta Universal Directory та Azure Active Directory (Azure AD). AWS SSO дозволяє вибирати атрибути користувача, наприклад центр витрат, посаду або мову, на основі джерела ідентифікаційних даних, а потім використовувати їх для керування доступом до AWS на основі атрибутів [13].

Єдиний вхід у AWS (AWS SSO) – це місце, де один раз створюється або

під’єднується посвідчення співробітників у AWS і централізовано керується доступом у своїй організації AWS. Можна керувати доступом лише до своїх облікових записів AWS або хмарних програм. Є можливість створювати посвідчення користувачів безпосередньо в AWS SSO, або можна завантажити їх зі свого Microsoft Active Directory або стандартного постачальника ідентифікаційних даних, наприклад Okta Universal Directory або Azure AD. Завдяки AWS SSO ви отримуєте уніфікований досвід адміністрування для визначення, налаштування та призначення детального доступу. Корпоративні співробітники отримують портал користувачів для доступу до всіх призначених їм облікових записів AWS, екземплярів Windows EC2 Amazon або хмарних програм. AWS SSO можна гнучко налаштувати для роботи разом із керуванням доступом до облікового запису AWS через AWS IAM або замінити його [14].

Розпочати роботу з AWS SSO легко. За допомогою лише кількох кліків на консолі керування можна підключити AWS SSO до наявного джерела ідентифікації та налаштувати дозволи, які надають користувачам доступ до призначених їм облікових записів AWS, хмарних додатків та інших програм на основі SAML, які додаються до AWS SSO [14].

Центральне місце для створення або об’єднання ідентифікаторів користувачів. Є можливість створити ідентифікатори та групи користувачів у AWS SSO. Або можна підключитися до наявних користувачів і груп із доменних служб Microsoft Active Directory, Okta Universal Directory, Azure AD або іншого постачальника ідентифікаційних даних на основі стандартів. У будь-якому випадку ви керуєте та автентифікуєте користувачів там, де хочете, а AWS SSO авторизує доступ до облікових записів AWS, хмарних додатків та інших програм на основі SAML, які додаються до AWS SSO.

Керування доступом до кількох облікових записів AWS з одного місця. Завдяки інтеграції організацій AWS, AWS SSO дає змогу керувати доступом до кількох облікових записів без додаткового налаштування в окремих облікових записах. Можна призначати дозволи користувачам на основі загальних робочих функцій, налаштовувати їх відповідно до ваших конкретних вимог безпеки та

призначати детальні дозволи в окремих облікових записах, до яких їм потрібен доступ. AWS SSO також дозволяє використовувати атрибути користувача, такі як центр витрат, назва або місцевий стандарт, для контролю доступу на основі атрибутів (ABAC).

Керування доступом до хмарних додатків. Завдяки єдиному входу AWS можна легко контролювати, хто має доступ до корпоративних хмарних програм. Користувачі можуть використовувати свої облікові дані каталогу для входу на свій веб-портал користувачів AWS SSO і отримати доступ одним клацанням миші до призначених їм програм, як-от Amazon SageMaker Studio, AWS Systems Manager Change Manager, а також хмарних додатків на основі стандартів, включаючи Salesforce, Box і Microsoft 365.

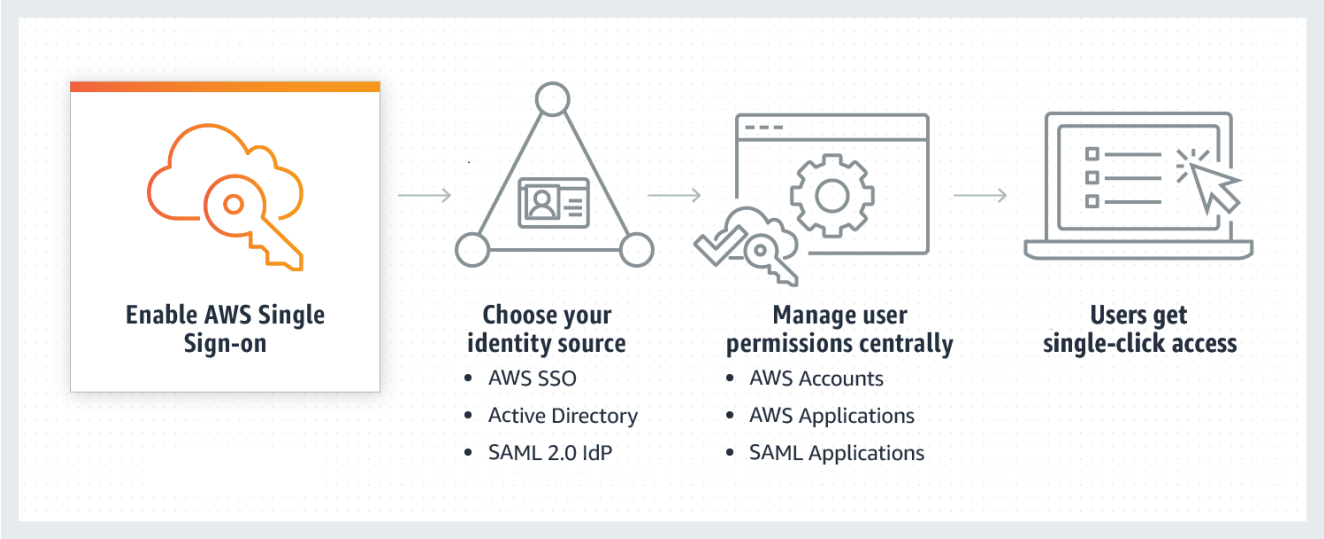

Рис. 2.6. Принцип функціонування AWS SSO [14]

AWS Single Sign-On (SSO) дозволяє легко централізовано керувати доступом до кількох облікових записів AWS і бізнес-додатків і надає користувачам доступ до всіх призначених їм облікових записів і програм з одного місця. Завдяки AWS SSO можна легко централізовано керувати доступом і дозволами користувачів до всіх своїх облікових записів в організаціях AWS. SSO автоматично налаштовує та підтримує всі необхідні дозволи для ваших облікових записів, не вимагаючи додаткового налаштування в окремих облікових записах. Існує можливість призначати дозволи користувача на основі загальних функцій

роботи та налаштовувати ці дозволи відповідно до конкретних вимог безпеки. AWS SSO також включає вбудовану інтеграцію з багатьма бізнес-додатками, такими як Salesforce, Box і Microsoft 365.

За допомогою AWS SSO можна створювати ідентифікаційні дані користувачів і керувати ними в сховищі ідентифікаційних даних AWS SSO або легко підключатися до наявного джерела посвідчень, зокрема Microsoft Active Directory, Okta Universal Directory і Azure Active Directory (Azure AD). AWS SSO дозволяє вибирати атрибути користувача, такі як центр витрат, назва або місцевість, із джерела ідентифікації, а потім використовувати їх для контролю доступу на основі атрибутів у AWS.

Можна підключити AWS SSO до свого існуючого джерела ідентифікації та налаштувати дозволи, які надають вашим користувачам доступ до призначених облікових записів організацій AWS та сотень попередньо налаштованих хмарних додатків, і все це з одного порталу користувача.

AWS SSO інтегровано з AWS Organizations, що дозволяє вибрати один або кілька облікових записів у вашій організації та надати користувачам доступ до цих облікових записів. AWS SSO базується на ролях і політиках керування ідентифікацією та доступом AWS (IAM), щоб допомогти вам централізовано керувати доступом до всіх облікових записів AWS в організації AWS. Додаткова конфігурація в індивідуальних облікових записах не потрібна. Лише кількома кліками ви можете надати користувачам доступ до всіх облікових записів AWS, які використовуються для програми або команди.

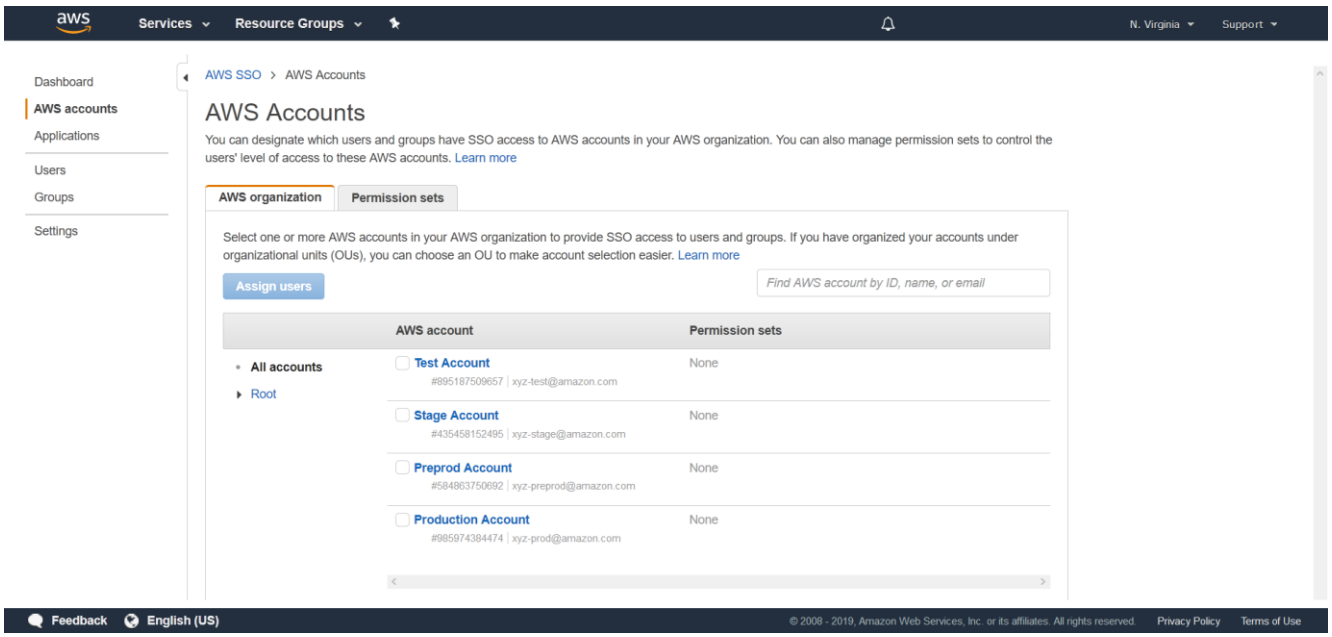

Рис. 2.7. Інтерфейс керування доступом користувачів до облікових записів [14]

За допомогою системи єдиного входу (SSO) AWS ви можете централізовано керувати доступом SSO для кількох облікових записів AWS. Коли користувачі входять на свої персоналізовані портали користувачів, вони бачитимуть усі призначені їм ролі в облікових записах AWS в одному місці.

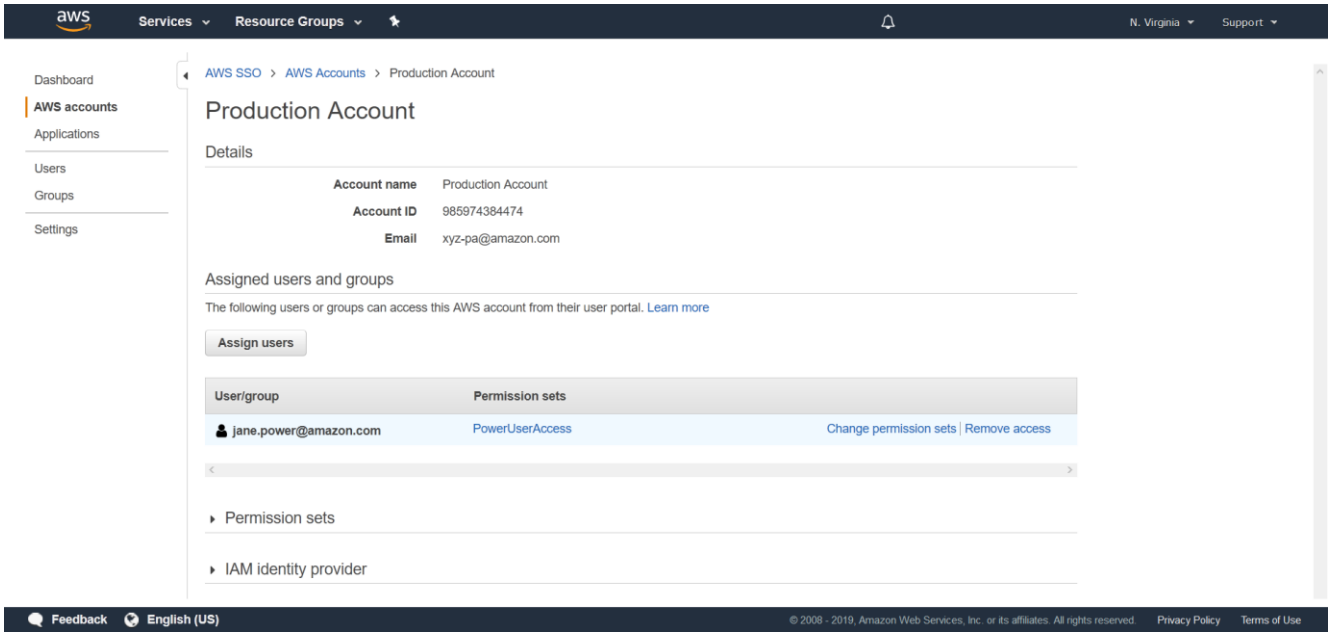

Рис. 2.8. Інтерфейс керування доступом SSO для кількох облікових записів AWS [14]

AWS SSO спрощує створення та використання детальних дозволів для вашої робочої сили на основі атрибутів користувача, визначених у вашому

джерелі ідентифікації AWS SSO. AWS SSO дозволяє вибрати кілька атрибутів, наприклад, центр витрат, назву або місцевість, а потім використовувати їх для контролю доступу на основі атрибутів (ABAC), щоб спростити та централізувати адміністрування доступу. Ви можете визначити дозволи один раз для всієї організації AWS, а потім надати, скасувати або змінити доступ AWS, просто змінивши атрибути у джерелі ідентифікації.

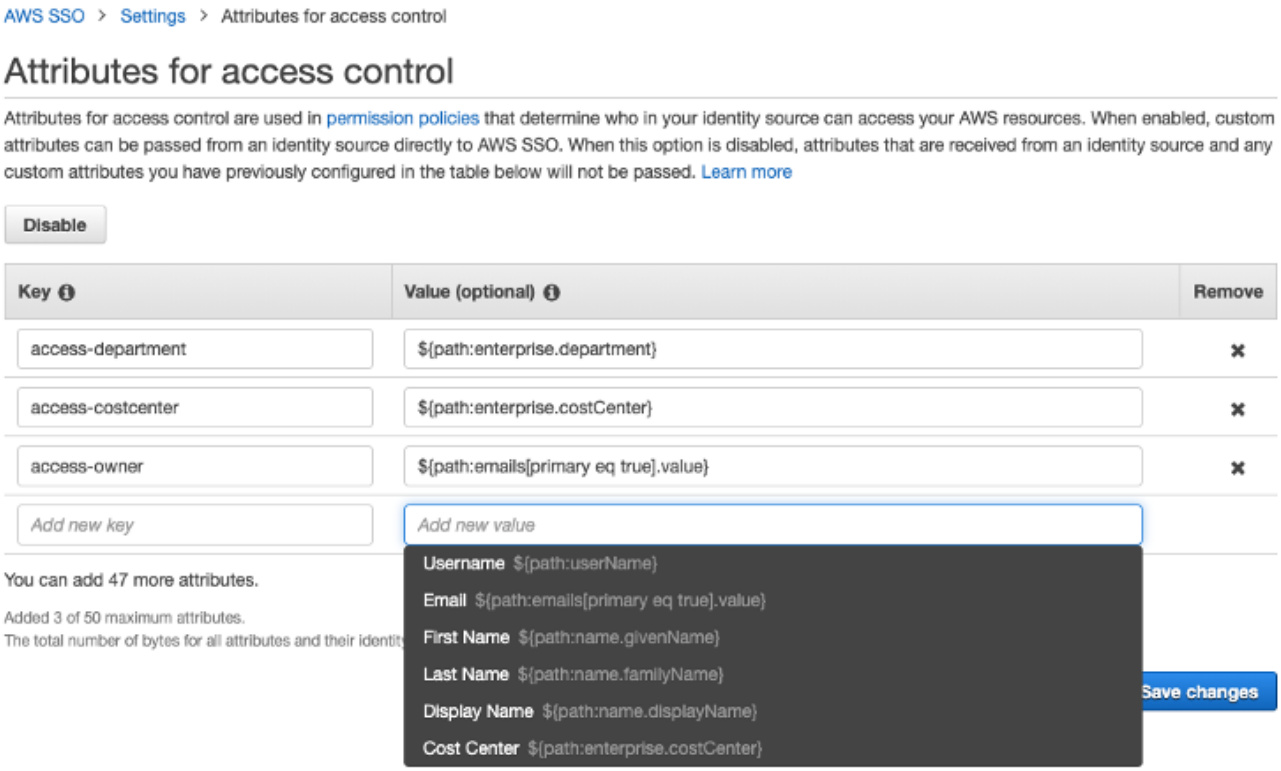

Рис. 2.9. Інтерфейс Контроль доступу на основі атрибутів [14]

З AWS SSO можна використовувати на основі стандартів потужні можливості автентифікації для всіх ваших користувачів у всіх джерелах ідентифікації. Якщо ви використовуєте підтримуваний ідентифікатор SAML 2.0 як джерело ідентифікації, ви можете увімкнути можливості багатофакторної автентифікації (MFA) вашого постачальника. Якщо ви використовуєте Active Directory або AWS SSO як джерело ідентифікації, AWS SSO підтримує специфікацію веб-автентифікації, щоб допомогти вам захистити доступ користувачів до облікових записів AWS і бізнес-додатків за допомогою ключів безпеки з підтримкою FIDO, таких як YubiKey, і вбудованих біометричних

автентифікаторів, наприклад, Touch ID на Apple MacBook і розпізнавання обличчя на ПК. Ви також можете ввімкнути одноразові паролі (TOTP) за допомогою програм для автентифікації, таких як Google Authenticator або Twilio Authy. AWS SSO дає змогу застосовувати MFA для всіх ваших користувачів, включаючи вимогу, щоб користувачі налаштовували пристрої MFA під час входу [14].

AWS SSO пропонує вам вбудовані інтеграції SSO з багатьма бізнес-додатками, включаючи Salesforce, Box і Microsoft 365. Ви можете легко налаштувати доступ SSO до цих програм, дотримуючись покрокових інструкцій. AWS SSO допоможе вам ввести необхідні URL-адреси, сертифікати та метадані. Повний список бізнес-програм, попередньо інтегрованих з AWS SSO, див. у AWS SSO Cloud Applications [14].

За допомогою майстра конфігурації програми AWS SSO ви можете створити інтеграцію єдиного входу до програм із підтримкою Security Assertion Markup Language (SAML) 2.0. Майстер конфігурації програми допомагає вибрати та відформатувати інформацію для надсилання програм, щоб увімкнути доступ SSO. Наприклад, ви можете створити атрибут SAML для імені користувача та вказати формат атрибута на основі електронної адреси користувача з його профілю AD [14].

Отже, AWS Single Sign-On дозволяє легко централізовано керувати доступом до кількох облікових записів AWS і бізнес-додатків та надає користувачам доступ до всіх призначених їм облікових записів і програм з одного місця, що забезпечує захищеність корпоративних даних.

3 ПОРЯДОК ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ХМАРНИХ СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES

3.1. Порядок розгортання рішення AWS IAM

AWS Identity and Access Management (IAM) допомагає безпечно контролювати доступ до Amazon Web Services (AWS) і ресурсів вашого облікового запису. IAM також може зберігати облікові дані вашого облікового запису конфіденційними. За допомогою IAM ви можете створити кількох користувачів IAM під парасолькою свого облікового запису AWS або ввімкнути тимчасовий доступ через об’єднання ідентифікаційних даних із корпоративним каталогом. У деяких випадках ви також можете ввімкнути доступ до ресурсів в облікових записах AWS.

Однак без IAM необхідно створити кілька облікових записів AWS – кожен із власними виставленнями рахунків і підписками на продукти AWS – або співробітники повинні надати доступ до облікових даних безпеки одного облікового запису AWS. Крім того, без IAM не можна контролювати завдання, які може виконувати певний користувач або система, і ресурси AWS, які вони можуть використовувати [12].

На рис. 3.1. показано простий приклад облікового запису AWS з трьома групами. Група – це сукупність користувачів, які мають подібні обов’язки. У цьому прикладі одна група призначена для адміністраторів (вона називається Адміністратори). Також є група розробників і тест група. Кожна група має кілька користувачів. Кожен користувач може бути більш ніж в одній групі, хоча малюнок цього не ілюструє. Не можна розміщувати групи в інших групах. Необхідно використовувати політику для надання дозволів групам [12].

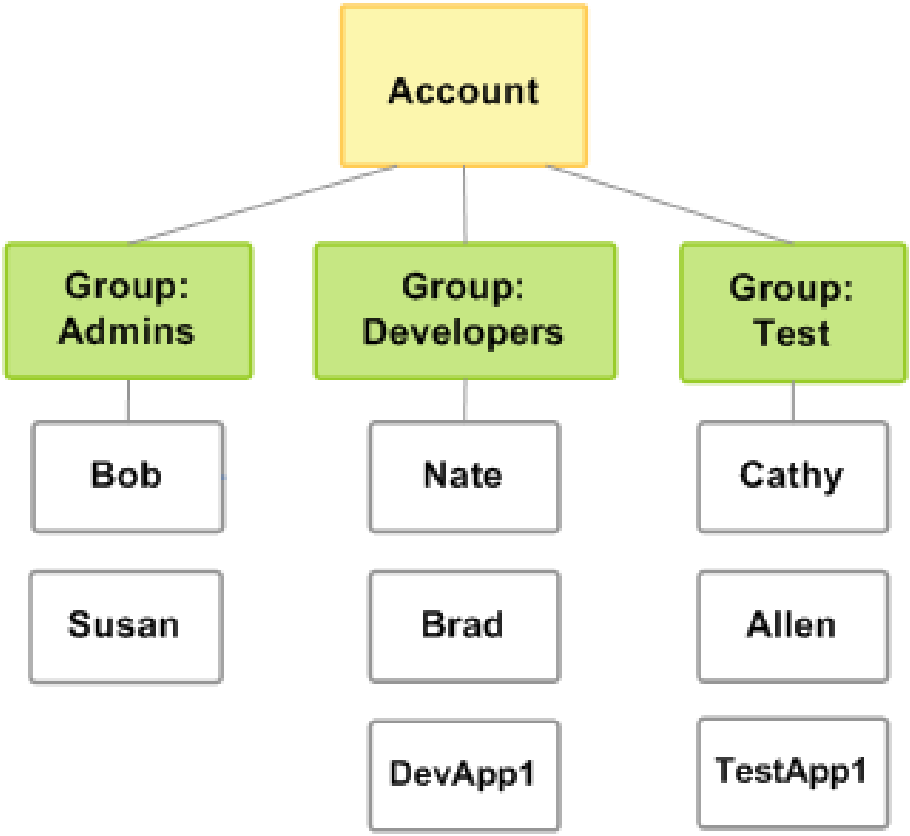

Рис. 3.1. Приклад облікового запису AWS з трьома групами [12]

У наведеній нижче процедурі ви будете виконувати такі завдання [12]:

створіть групу адміністраторів і надайте групі дозвіл на доступ до всіх ресурсів вашого облікового запису AWS;

створіть собі користувача та додайте його до групи адміністраторів;

створіть пароль для свого користувача, щоб ви могли ввійти в Консоль керування AWS.

Групі адміністраторів надається дозвіл на доступ до всіх доступних ресурсів облікового запису AWS. Доступними ресурсами є будь-які продукти AWS, які ви використовуєте або на які ви зареєструвалися. Користувачі групи адміністраторів також можуть отримати доступ до інформації вашого облікового запису AWS, за винятком облікових даних вашого облікового запису AWS.

Створення першого користувача-адміністратора IAM і групи користувачів. Як найкраща практика, не використовуйте користувача root облікового запису AWS для виконання будь-яких завдань, де це не потрібно.

Натомість створіть нового користувача IAM для кожної особи, якій потрібен доступ адміністратора. Потім зробіть цих користувачів адміністраторами, помістивши користувачів у групу користувачів «Адміністратори», до якої ви приєднаєте керовану політику *AdministratorAccess*.

Після цього користувачі в групі адміністраторів мають налаштувати групи користувачів, користувачів тощо для облікового запису AWS. Вся подальша взаємодія має здійснюватися через користувачів облікового запису AWS та їхні власні ключі, а не через користувача *root*. Однак для виконання деяких завдань керування обліковими записами та службами необхідно ввійти, використовуючи облікові дані користувача *root*.

Приклад делегування доступу до платіжної консолі.

Власники облікових записів AWS можуть делегувати доступ певним користувачам IAM, яким потрібно переглядати або керувати даними AWS Billing & Cost Management для облікового запису AWS. Наведені нижче інструкції допоможуть налаштувати попередньо перевірений сценарій. Цей сценарій допоможе отримати практичний досвід налаштування дозволів на виставлення рахунків, не турбуючись про вплив на основний робочий обліковий запис AWS. Якщо ви додаєте керовану політику до своїх користувачів IAM, спочатку потрібно активувати доступ до консолі AWS Billing and Cost Management на кроці 1. Цей робочий процес складається з чотирьох основних кроків (рис. 3.2).

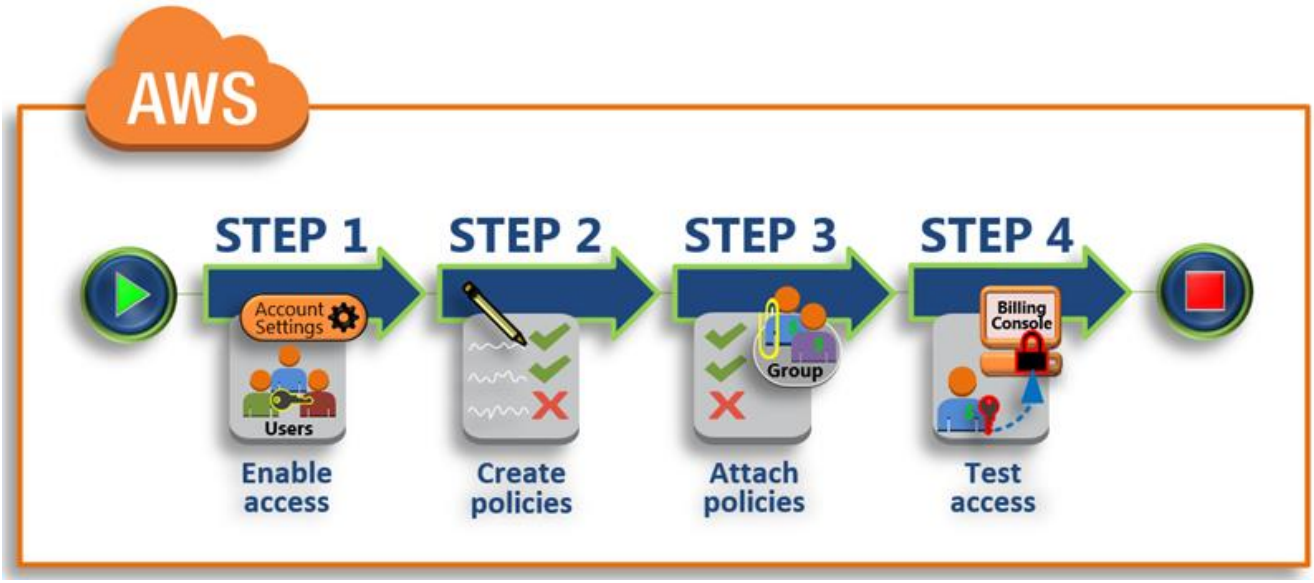

Рис. 3.2. Кроки делегування доступу до платіжної консолі [12]

Крок 1. Активуйте доступ до платіжних даних у своєму тестовому обліковому записі AWS.

Якщо створюється один обліковий запис AWS, лише власник облікового запису AWS (кореневий користувач облікового запису AWS) має доступ до перегляду платіжної інформації та керування нею. Користувачі IAM не можуть отримати доступ до платіжних даних, доки власник облікового запису не активує доступ до IAM, а також не додасть політики, які забезпечують дії щодо платежів для користувача або ролі.

Якщо створюється обліковий запис члена за допомогою організацій AWS, ця функція ввімкнена за замовчуванням.

Крок 2. Створіть правила IAM, які надають дозволи на платіжні дані.

Після ввімкнення доступу до виставлення рахунків в обліковому записі ви все одно повинні явно надати доступ до платіжних даних певним користувачам або групам користувачів IAM. Цей доступ надається за допомогою політики, керованої клієнтом.

Крок 3. Додайте правила оплати до своїх груп користувачів.

Коли ви приєднуєте політику до групи користувачів, усі члени цієї групи користувачів отримують повний набір дозволів доступу, пов’язаних з цією політикою. У цьому сценарії ви долучаєте нові політики оплати до груп користувачів, які містять лише тих користувачів, яким потрібен доступ до платежів.

Крок 4. Перевірте доступ до платіжної консолі.

Виконавши основні завдання, ви готові протестувати політику. Тестування гарантує, що політика працює так, як ви хочете.

Приклад делегування доступу до облікових записів AWS за допомогою ролей IAM.

Ролі IAM і політика на основі ресурсів делегують доступ між обліковими записами лише в межах одного розділу.

Розробники можуть використовувати роль у Консолі керування AWS для доступу до *productionapp* сегмента в робочому обліковому записі. Вони також

можуть отримати доступ до сегмента за допомогою викликів API, автентифікованих за допомогою тимчасових облікових даних, наданих роллю.

Цей робочий процес складається з трьох основних кроків (рис. 3.3).

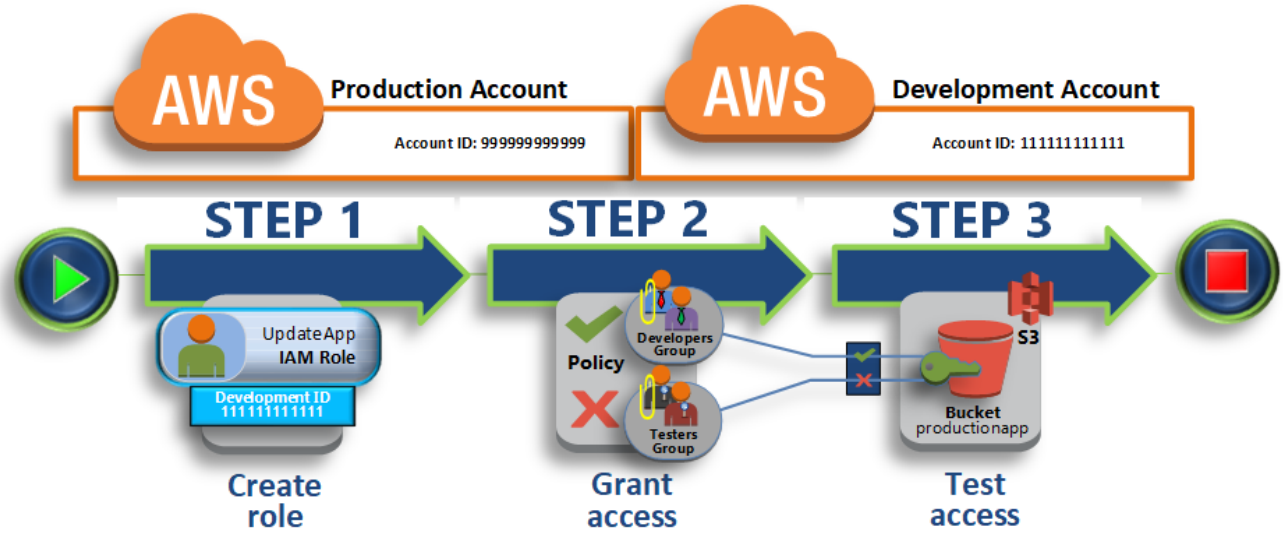

Рис. 3.3. Кроки делегування доступу до облікових записів AWS за допомогою ролей IAM [12]

Крок 1. Створіть роль у виробничому обліковому записі.

По-перше, ви використовуєте Консоль керування AWS, щоб встановити довіру між робочим обліковим записом (ідентифікаційний номер 999999999999) та обліковим записом розробки (ідентифікаційний номер 111111111111). Ви починаєте зі створення ролі IAM з назвою *UpdateApp*. Коли ви створюєте роль, ви визначаєте обліковий запис розробника як надійну сутність і вказуєте політику дозволів, яка дозволяє довіреним користувачам оновлювати *productionapp* сегмент.

Крок 2: Надайте доступ до ролі.

На цьому кроці ви змінюєте групову політику IAM, щоб заборонити тестувальникам доступ до *UpdateApp* ролі. Оскільки тестувальники мають доступ *PowerUser* у цьому сценарії, і ви повинні явно заборонити можливість використовувати цю роль.

Крок 3. Перевірте доступ, міняючи ролі.

Нарешті, як розробник, ви використовуєте *UpdateApp* роль для оновлення

productionapp сегмента в робочому обліковому записі. Ви бачите, як отримати доступ до ролі через консоль AWS, інтерфейс командної команди AWS та API.

Приклад створення і додавання першої політику, керованої клієнтом.

Ми можемо використовувати консоль керування AWS, щоб створити політику, керовану клієнтом, а потім приєднати цю політику до користувача IAM у вашому обліковому записі AWS. Створена політика дозволяє тестовому користувачеві IAM входити безпосередньо в Консоль керування AWS з дозволами лише на читання.

Цей робочий процес складається з трьох основних кроків (рис. 3.4).

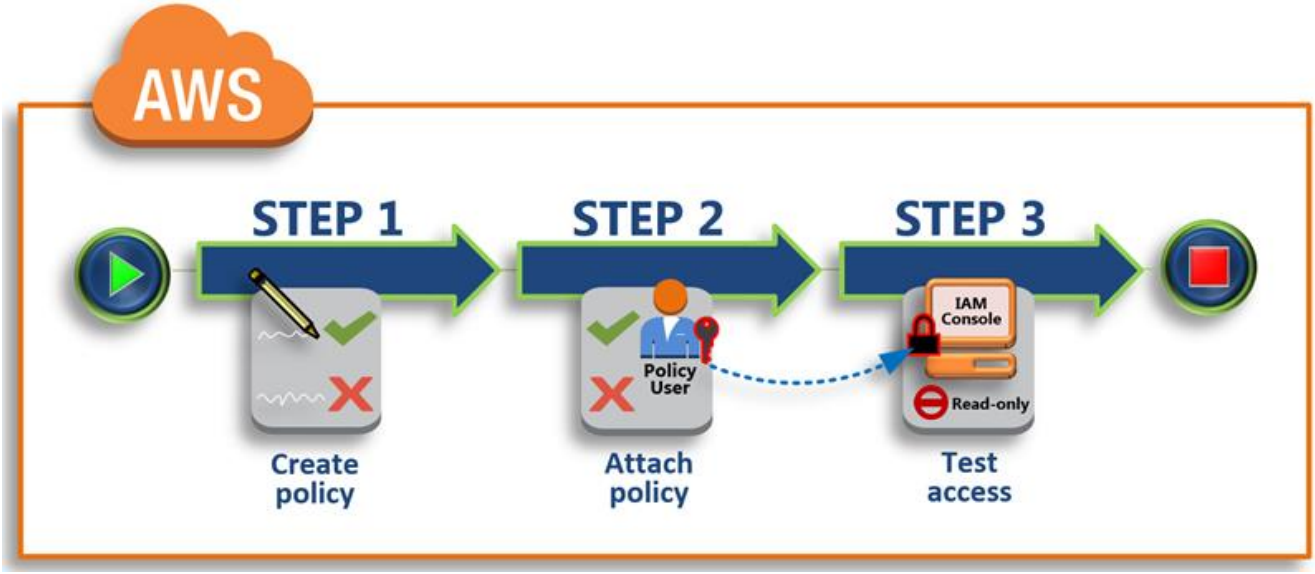

Рис. 3.4. Кроки створення і додавання першої політику, керованої клієнтом [12]

Крок 1. Створіть політику.

За замовчуванням користувачі IAM не мають дозволів на будь-які дії. Вони не можуть отримати доступ до Консолі керування AWS або керувати даними, якщо ви не дозволите це. На цьому кроці ви створюєте політику, керовану клієнтом, яка дозволяє будь-якому підключеному користувачеві входити на консоль.

Крок 2. Прикріпіть політику.

Коли ви приєднуєте політику до користувача, він успадковує всі дозволи доступу, пов’язані з цією політикою. На цьому кроці ви приєднуєте нову політику до тестового облікового запису користувача.

Крок 3. Перевірте доступ користувача.

Коли політику буде додано, ви можете ввійти як користувач і перевірити політику.

3.2. Технологія застосування рішення AWS IAM

Розглянемо політики та дозволи в AWS IAM.

Керування доступом в AWS здійснюється, створюючи політики та приєднуючи їх до ідентифікаційних даних IAM (користувачів, груп користувачів або ролей) або ресурсів AWS. Політика – це об’єкт в AWS, який, пов’язаний із ідентифікатором або ресурсом, визначає їхні дозволи. AWS оцінює ці політики, коли принципал IAM (користувач або роль) робить запит. Дозволи в політиках визначають, дозволено чи відхилено запит. Більшість політик зберігаються в AWS як документи JSON. AWS підтримує шість типів політик, які розглядаються нижче.

Політики IAM визначають дозволи для дії незалежно від методу, який ви використовуєте для виконання операції. Наприклад, якщо політика дозволяє *GetUser* дії, то користувач із цією політикою може отримати інформацію про користувача з Консолі керування AWS, AWS CLI або AWS API. Коли ви створюєте користувача IAM, ви можете дозволити консольний або програмний доступ. Якщо доступ до консолі дозволено, користувач IAM може ввійти на консоль за допомогою імені користувача та пароля. Або якщо програмний доступ дозволено, користувач може використовувати ключі доступу для роботи з CLI або API.

Розглянемо типи політик.

Для використання в AWS доступні наступні типи політики, перераховані в порядку від найбільш часто використовуваних до менш часто використовуваних. Щоб дізнатися більше, перегляньте розділи нижче для кожного типу політики [12].

Політики на основі ідентифікаційних даних – додадаються керовані та

вбудовані політики до ідентифікаційних даних IAM (користувачів, груп, до яких належать користувачі, або ролей). Політики на основі ідентифікаційних даних надають дозволи для ідентифікації.

Політики на основі ресурсів – додаються вбудовані політики до ресурсів. Найпоширенішими прикладами політик на основі ресурсів є політики сегмента Amazon S3 і політики довіри ролей IAM. Політики на основі ресурсів надають дозволи принципалу, зазначеному в політиці. Принципали можуть бути в тому ж обліковому записі, що й ресурс, або в інших облікових записах [12].

Межі дозволів – використовується керована політика як межа дозволів для сутності IAM (користувача чи ролі). Ця політика визначає максимальні дозволи, які політика на основі ідентифікаційних даних може надати сутності, але не надає дозволів. Межі дозволів не визначають максимальні дозволи, які політика на основі ресурсів може надати об’єкту.

SCP організацій. Використовується політика керування службами AWS Organizations (SCP), щоб визначити максимальні дозволи для членів облікового запису організації чи організаційного підрозділу (OU). SCP обмежують дозволи, які політика на основі ідентифікаційних даних або політика на основі ресурсів надають сутностям (користувачам або ролям) в обліковому записі, але не надають дозволів [12].

Списки контролю доступу (ACL) – використовуються списки керування доступом, щоб контролювати, які принципали в інших облікових записах можуть отримати доступ до ресурсу, до якого приєднано ACL. ACL подібні до політик на основі ресурсів, хоча це єдиний тип політики, який не використовує структуру документа політики JSON. ACL – це політики дозволів для кількох облікових записів, які надають дозволи вказаному принципалу. ACL не може надавати дозволи об’єктам в межах одного облікового запису [12].

Політики сеансу застосовуються, коли ви використовуєте AWS CLI або AWS API, щоб взяти на себе роль або як федеративний користувач. Політики сеансу обмежують дозволи, які надають сеансу політика на основі ідентичності ролі або користувача. Політики сеансу обмежують дозволи для створеного сеансу,

але не надають дозволи.

Політики на основі ідентифікаційних даних – це документи політики дозволів JSON, які контролюють, які дії може виконувати особа (користувачі, групи користувачів і ролі), на яких ресурсах та за яких умов. Політику на основі ідентифікації можна додатково класифікувати:

керовані політики – окремі політики на основі ідентифікаційних даних, які можна приєднати до кількох користувачів, груп і ролей у своєму обліковому записі AWS. Існує два типи керованих політик:

керовані політики AWS – керовані політики, які створює та керує AWS;

політики, керовані клієнтом – керовані політики, які ви створюєте та керуєте у своєму обліковому записі AWS. Політики, керовані клієнтом, забезпечують більш точний контроль над вашими політиками, ніж політики AWS;

вбудовані політики – політики, які додаються безпосередньо до окремого користувача, групи чи ролі. Вбудовані політики підтримують строгі стосунки один на один між політикою та ідентифікатором. Вони видаляються, коли ви видаляєте ідентифікатор.

Політики на основі ресурсів – це документи політики JSON, які додаються до такого ресурсу, як сегмент Amazon S3. Ці політики надають зазначеному принципалу дозвіл виконувати певні дії над цим ресурсом і визначають, за яких умов це застосовується. Політики на основі ресурсів є вбудованими політиками. Немає політик на основі керованих ресурсів [12].

Щоб увімкнути доступ до кількох облікових записів, ви можете вказати весь обліковий запис або об’єкти IAM в іншому обліковому записі як основний у політиці на основі ресурсів. Додавання принципала для кількох облікових записів до політики на основі ресурсів – це лише половина встановлення довірчих відносин. Якщо принципал і ресурс знаходяться в окремих облікових записах AWS, ви також повинні використовувати політику на основі ідентифікації, щоб надати принципал доступ до ресурсу. Однак, якщо політика на основі ресурсів надає доступ до принципала в тому самому обліковому записі, додаткова політика на основі ідентифікації не потрібна [12].

Сервіс IAM підтримує лише один тип політики на основі ресурсів, яка називається політикою довіри ролі , який додається до ролі IAM. Роль IAM – це і ідентифікатор, і ресурс, який підтримує політику на основі ресурсів. З цієї причини до ролі IAM необхідно приєднати політику довіри та політику на основі ідентифікації. Політики довіри визначають, які основні об’єкти (облікові записи, користувачі, ролі та об’єднані користувачі) можуть взяти на себе цю роль [12].

Межа дозволів – це розширена функція, у якій встановлюється максимальні дозволи, які політика на основі ідентифікаційних даних може надати об’єкту IAM. Коли ви встановлюєте межі дозволів для об’єкта, об’єкт може виконувати лише ті дії, які дозволені як його політиками на основі ідентифікаційних даних, так і його межами дозволів. Політики на основі ресурсів, які визначають користувача або роль як принципала, не обмежені межами дозволів. Явна заборона в будь-якій із цих політик перекриває дозвіл [12].

Політики контролю послуг (SCP)/ AWS Organizations – це сервіс для групування облікових записів AWS, якими володіє ваша компанія, і централізованого керування ними. Якщо ви ввімкнете всі функції в організації, ви зможете застосувати політику керування послугами (SCP) до будь-якого або всіх своїх облікових записів. SCP – це політики JSON, які визначають максимальні дозволи для організації чи організаційного підрозділу (OU). SCP обмежує дозволи для об’єктів в облікових записах учасників, включаючи кожного користувача root облікового запису AWS. Явна заборона в будь-якій із цих політик перекриває дозвіл [12].

Списки контролю доступу (ACL) – це політики служби, які дозволяють контролювати, які принципали в іншому обліковому записі можуть отримати доступ до ресурсу. ACL не можна використовувати для керування доступом для принципала в межах одного облікового запису. ACL подібні до політик на основі ресурсів, хоча це єдиний тип політики, який не використовує формат документа політики JSON. Amazon S3, AWS WAF і Amazon VPC є прикладами служб, які підтримують списки керування доступом.

Політики сеансу – це розширені політики, які ви передаєте як параметр,

коли програмно створюєте тимчасовий сеанс для ролі або об’єднаного користувача. Дозволи для сеансу є перетином політик на основі ідентифікації для об’єкта IAM (користувача чи ролі), який використовується для створення сеансу, та політик сеансу. Дозволи також можуть виходити з політики на основі ресурсів. Явна заборона в будь-якій із цих політик перекриває дозвіл [12].

Ви можете створити сеанс ролі та передати політику сеансу програмно за допомогою операцій *AssumeRole*, *AssumeRoleWithSAML*, або *AssumeRoleWithWebIdentityAPI*. Ви можете передати один вбудований документ політики сеансу JSON за допомогою *Policy* параметра. За допомогою цього *PolicyArns* параметра можна вказати до 10 керованих політик сеансу.

Коли ви створюєте сеанс федеративного користувача, ви використовуєте ключі доступу користувача IAM для програмного виклику *GetFederationToken* операції API. Ви також повинні передати політику сеансу. Отримані дозволи сеансу є перетином політики на основі ідентифікації користувача IAM і політики сеансу.

Політика на основі ресурсів може вказувати ARN користувача або роль як принципала. У цьому випадку дозволи з політики на основі ресурсів додаються до політики на основі ролі або ідентифікації користувача перед створенням сеансу. Політика сеансу обмежує загальну кількість дозволів, наданих політикою на основі ресурсів і політикою на основі ідентифікаційних даних. Отримані дозволи сеансу є перетином політик сеансу та політики на основі ресурсів плюс перетин політик сеансу та політик на основі ідентифікаційних даних (рис. 3.4).

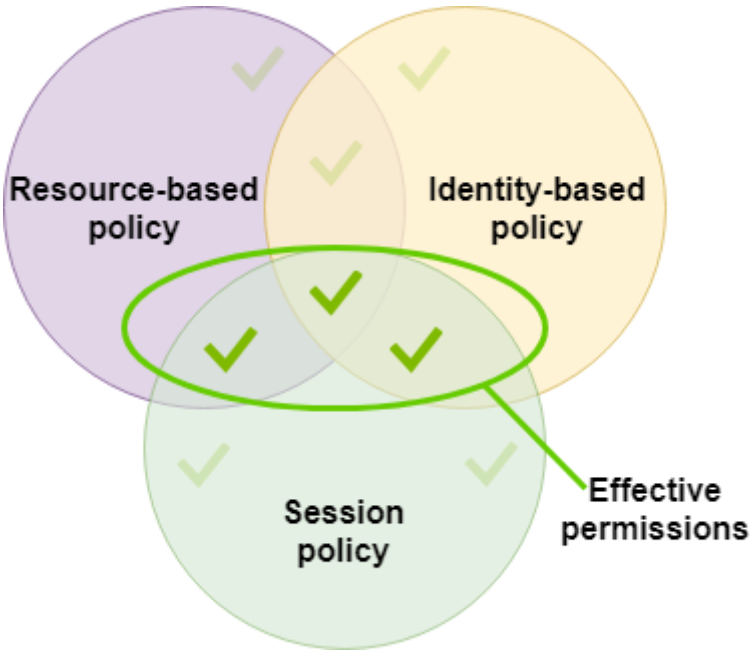

Рис. 3.4. Пояснення формування дозволу [12]

Політика на основі ресурсів може вказати ARN сеансу як принципала. У цьому випадку дозволи з політики на основі ресурсів додаються після створення сеансу. Дозволи політики на основі ресурсів не обмежені політикою сеансу. Отриманий сеанс має всі дозволи політики на основі ресурсів плюс перетин політики на основі ідентифікації та політики сеансу (рис. 3.5).

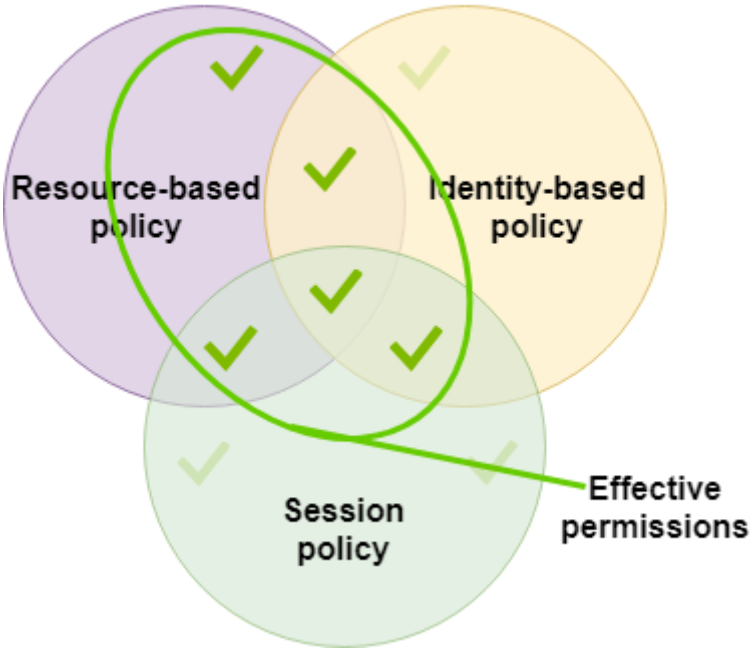

Рис. 3.5. Пояснення формування дозволу [12]

Межа дозволів може встановлювати максимальні дозволи для користувача або ролі, які використовуються для створення сеансу. У цьому випадку дозволи результуючого сеансу є перетином політики сеансу, межі дозволів і політики на основі ідентифікації. Однак межі дозволів не обмежують дозволи, надані політикою на основі ресурсів, яка визначає ARN результуючого сеансу (рис. 3.6).

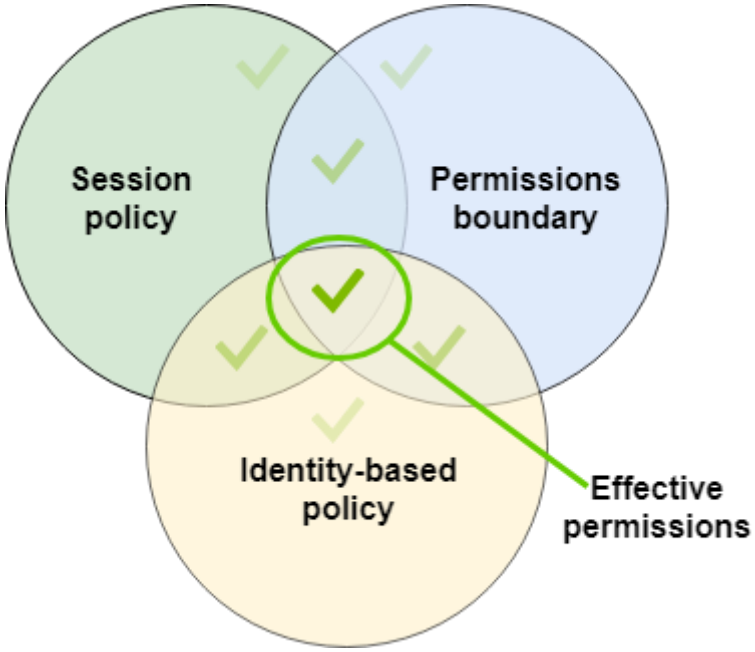

Рис. 3.6. Пояснення формування дозволу [12]

Розглянемо питання управління дозволами IAM.

За допомогою дозволів можна надавати доступ до ресурсів AWS. Дозволи надаються об’єктам IAM (користувачам, групам та ролям), при цьому за замовчуванням у цих об’єктів відсутні будь-які дозволи. Іншими словами, об’єкти IAM не можуть виконувати жодних дій на платформі AWS, доки їм не надані необхідні дозволи. Щоб надати об’єктам дозволу, можна призначити правило, яке визначатиме тип доступу, дії, які можуть бути виконані, а також ресурси, на яких можуть виконуватись певні дії. Крім того, можна вказати будь-які умови, які мають виконуватися для дозволу або заборони доступу [15].

Щоб призначити дозволи для користувача, групи, ролі або ресурсу, створіть політику, яка дозволить зазначити наступне [15].

Actions. Дозволені дії для сервісу AWS. Наприклад, можна дозволити користувачеві викликати дію Amazon S3 ListBucket. Будь-які дії, які ви явно не

дозволяєте виконувати, забороняються.

Resources. Ресурси AWS, для яких можна виконувати певні дії. Наприклад, список кошиків Amazon S3, для яких ви дозволяєте користувачеві виконувати дію ListBucket. Користувачі не можуть отримати доступ до тих ресурсів, для яких ви не надаєте дозволу.

Effect. Дозволяти або забороняти доступ. Оскільки за промовчанням доступ заборонено, ви зазвичай створюєте правила, які дозволяють певні дії.

Conditions. Умови, які мають виконуватися, щоб застосовувалася політика. Наприклад, можна дозволити доступ лише до певних корзин S3, якщо користувач підключається з певного діапазону IP-адрес або використовує при вході в систему багатофакторну автентифікацію.

Політики створюються за допомогою візуального редактора або у форматі JSON. Політика складається з одного або кількох виразів, кожен з яких описує один набір дозволів.

Рис. 3.7. Візуальний редактор дозволів [15]

Візуальний редактор проведе вас через надання дозволів за допомогою правил IAM без необхідності писати правила у форматі JSON (при цьому

можливість створювати та редагувати правила в JSON зберігається). Правило, показане на знімку екрана, було створено за допомогою візуального редактора. Воно надає дозвіл на п’ять дій Amazon S3 типу List та Read для кошика S3 та об’єктів у SampleBucket, префікс яких починається з MyPrefix (рис. 3.7) [15].

При використанні керування дозволами Консолі керування AWS можна переглянути інформацію про правила. У зведеній інформації про правило перераховані рівень доступу, ресурси та умови для кожного сервісу, визначеного у правилі (див. приклад на наведених нижче знімках екрана). Щоб було легше зрозуміти дозволи, визначені у правилі, дії кожного сервісу AWS розбиті на чотири категорії за рівнем доступу: List, Read, Write та Permissions management.

Service ▾	Access level	Resource	Request condition
Allow (10 of 94 services)			
CloudFormation	**Full**: List **Limited**: Read, Write	All resources	None
CloudWatch Logs	Full access	Multiple	None
EC2	**Full**: List **Limited**: Read	All resources	None
Elastic Beanstalk	Full access	All resources	elasticbeanstalk:InApplication = arn:aws:elasticbeanstalk:*:111122223333:application/Bank-Devl

Рис. 3.8. Чотири категорії дозволів за рівнем доступу [15]

Ми можемо вибрати певне правило під керуванням AWS або створити власне, використовуючи генератор правил.

3.3. Рекомендації щодо управління доступом користувачів до хмарних сервісів та ресурсів організації

Хмарні сервіси – зручне та ефективне вирішення безлічі завдань сучасного бізнесу. Використання співробітниками сервісів та баз даних, розгорнутих у ЦОД та хостингах провайдерів хмарних послуг, дозволяє знизити потреби у підтримці власного парку високопродуктивних серверів. Але при організації взаємодії користувачів з хмарними сервісами, питання забезпечення захисту та збереження конфіденційності даних, що передаються, стоїть не менш гостро, ніж при будь-

яких інших способах взаємодії між клієнтами і сервером додатків або баз даних.

Необхідно відмітити, що порушення даних та їх витік є основними проблемами безпеки у хмарі. Головна причина – нехтування можливостями захисту інформації.

Основними рекомендаціями щодо забезпечення безпеки даних при використанні хмарних сервісів є:

настроїти резервне копіювання;

вибрати надійних постачальників послуг з ЦОД не нижче рівня TIER III;

системно оцінювати рівень безпеки;

встановити надійні політики керування доступом;

створити план аварійного відновлення;

проведення роз'яснювальної роботи зі співробітниками на предмет, що можна робити у хмарі, а що не можна.

Розглянемо дані рекомендації більш детально.

Найчастіше резервне копіювання даних є найбільш ефективним способом підвищити безпеку хмарних сервісів. Щоб правильно його налаштувати, потрібно чітко розуміти, які дані є критично важливими. Можна створювати бекапи окремих файлів, баз даних чи всієї системи.

Втратити дані можна через нехтування заходами безпеки постачальниками хмарних послуг. Відповідальні провайдери надають сервери з налаштованим шифруванням, антивірусом і фаєрволом. Самі машини зберігають у надійних Центрах обробки даних рівня TIER III. Це означає, що ризик пожежі, затоплення, поломки зведений до мінімуму.

Хмарні послуги регулярно модернізують. Оновлення допомагають підвищити продуктивність, усувають недоліки. Але ж вони несуть у собі й нові дірки у безпеці. Потрібно регулярно перевіряти трафік та мережеву активність, особливо після встановлення або оновлення програмного забезпечення. Найкраще зарекомендувало себе автоматичне виявлення загроз із використанням штучного інтелекту.

Необхідно розробляти та втілювати надійні політики керування доступом.

Треба дозволяти доступ лише тим працівникам, які його потребують. Переконайтеся, що ви можете закрити цей доступ у будь-який момент. Для додаткового рівня безпеки даних у хмарі використовуйте методи багатофакторної або біометричної автентифікації.

Втрата доступу до хмарних послуг є серйозною загрозою безпеці. Більше того, будь-які простої призведуть до серйозних фінансових втрат. Щоб уникнути втрати даних та мінімізувати час простою після збою, необхідно розробляти План аварійного відновлення та переконатися, що відповідальні співробітники цей план знають.

Усі працівники, які мають доступ до хмарних сервісів, повинні мати базові уявлення про кібербезпеку. Багато хто до цих пір може відкривати підозрілі імейли або переходити за фішинговими посиланнями. У деяких випадках знадобиться налаштувати обмеження трафіку, щоб унеможливити перехід на сторонні сайти.

Необхідно розуміти, що зловмисники постійно використовують людський фактор для злому та крадіжки даних у хмарі, а саме:

вивчають структуру підприємства на наявність слабких місць (експлойтів);

після ідентифікації жертви знаходять спосіб наблизитися до людини – це включає виявлення облікових записів в соціальних мережах, інтересів і можливих недоліків;

після цього жертву змушують надати доступ до хмарного облікового запису – є два способи зробити це: через шкідливі програми, за допомогою соціальної інженерії (завоювавши довіру).

Незважаючи на те, що Інтернет існує давно, багато хто із співробітників ставиться до кібератак безтурботно та постійно порушують політики безпеки хмарних сервісів. Це вимагає постійного контролю за роботою співробітників з хмарними ресурсами організацій.

Неправильні налаштування безпеки хмарної інфраструктури зроблять марною навіть найпродуманішу стратегію захисту. Тому не можна:

встановлювати стандартні параметри безпеки. Абсолютно всі вони мають

бути персоналізовані під потреби орендаря;

ігнорувати налаштування прав доступу. Стороння людина може ненавмисно отримати доступ до конфіденційних даних;

не розмежовувати дані щодо важливості. Якщо конфіденційна інформація залишається відкритою, до неї можуть отримати доступ зловмисники.

Вибираючи для бізнесу рішення щодо безпеки хмарних сервісів, важливо розуміти, які вимоги висувають регуляторні органи та які загрози реально існують у тій чи іншій сфері. Особливо, коли бізнес працює з чутливими даними, наприклад, платіжними засобами чи медичною інформацією. Або у країні, законодавство якої вимагає зберігати дані громадян лише на своїй території.

Управління доступом до додатків має здійснюється на основі групових політик, що унеможливлює несанкціоноване використання співробітником своїх облікових даних у разі звільнення.

Поява нових можливостей завдяки хмарним сервісам і таким кінцевим пристроям, як смартфони або планшетні ПК, дозволяє реалізувати економічно більш вигідну та гнучку альтернативну модель, але водночас ускладнює забезпечення належного рівня захисту даних та додатків (як на оперативному, так і на технічному рівні). Гнучкий та універсальний доступ до корпоративних додатків у хмарі вимагає впровадження нової цілісної концепції безпеки ІТ, що охоплює інфраструктуру, програми, з’єднання та насамперед захищений доступ до хмарних сервісів та ресурсів.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми управління доступом користувачів до хмарних сервісів та ресурсів організації як складової частини забезпечення кібербезпеки її інформаційної системи, встановлена сутність завдань управління доступом.

Amazon Web Services (AWS) – це найпоширеніша у світі хмарна платформа з найширшими можливостями, що надає понад 200 повнофункціональних сервісів для центрів обробки даних. Тому, AWS широко застосовується у сучасних організаціях. Даний момент визначає необхідність централізованого управління доступом користувачів до хмарних сервісів та ресурсів організації.

Проаналізовано існуючі технології управління доступом користувачів до хмарних сервісів та ресурсів організації. Досліджена технологія управління доступом користувачів до хмарних сервісів та ресурсів організації на прикладі Amazon Web Services.

Визначено методи та засоби управління доступом користувачів до хмарних сервісів та ресурсів Amazon Web Services. Встановлено основні функції та принципи роботи сервісу AWS IAM. AWS IAM забезпечує точний контроль доступу у всіх сервісах AWS. За допомогою IAM надається доступ до певних сервісів та ресурсів за відповідними умовами. Завдяки політикам IAM здійснюється управління дозволами для співробітників та систем, надаючи дозволи з найменшими привілеями. Використовуючи політики IAM, надається доступ до певних API сервісів та ресурсів AWS. Також визначаються конкретні умови для надання доступу, наприклад, певна організація AWS або використання певного сервісу AWS.

Визначена сутність моделі управління доступом користувачів на основі атрибутів в AWS IAM. Управління доступом на основі атрибутів (ABAC) – це стратегія авторизації для створення деталізованих дозволів на базі атрибутів користувача, таких як відділ, робоча роль і назва команди. За допомогою ABAC

можна скоротити кількість дозволів, необхідних для точного керування обліковим записом AWS.

Досліджено призначення, можливості та функції централізованого управління доступом до облікових записів та додатків AWS Single Sign-On. Даний сервіс забезпечує створення або підключення посвідчення співробітників і централізовано керуєте доступом всієї організації до AWS. Контролюється як доступ тільки до своїх облікових записів AWS, так і до хмарних додатків. AWS Single Sign-On – це єдиний адміністративний інтерфейс для точного визначення, налаштування та надання доступу. Корпоративні користувачі отримують портал користувача для доступу до всіх призначених облікових записів AWS або хмарних додатків.

У роботі запропоновано порядок розгортання та застосування технології управління доступом користувачів до хмарних сервісів та ресурсів на прикладі рішення AWS IAM. Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології управління доступом користувачів до хмарних сервісів та ресурсів організації.

Таким чином, правильна реалізація технології управління доступом користувачів до хмарних сервісів та ресурсів організації як складової частини забезпечення кібербезпеки її інформаційної системи, має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Morey J. Haber, Darran Rolls. Identity Attack Vectors. Implementing an Effective Identity and Access Management Solution. Apress Media. 2020. 205 p.

2. Michael Schwartz, Maciej Machulak. Securing the Perimeter. Deploying Identity and Access Management with Free Open Source Software. 2018. 383 p.

3. Michael Wittig, Andreas Wittig, foreword by Ben Whaley. Amazon Web Services in Action, Second Edition. Manning Publications Co. 2019. 530 p.

4. Хмарні тренди: як розвиватимуться cloud-технології та навіщо вони бізнесу. Kyivstar Business Hub. 11 березня 2021 р. https://hub.kyivstar.ua/news/hmarni-trendi-yak-rozvivatimutisya-cloud-tehnologii-ta-navishho-voni-biznesu/.

5. Gartner. Magic Quadrant for Cloud Infrastructure and Platform Services. Published 27 July 2021 https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb.

6. Hu, C., Ferraiolo, D., Kuhn, D., Schnitzer, A., Sandlin, K., Miller, R. and Scarfone, K. (2019), Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927500 (Accessed November 27, 2021).

7. Cloud computing with AWS. https://aws.amazon.com/what-is-aws/?nc1=h_ls.

8. Designing a modern IAM program for your business. IBM Security. September 2020. https://www.ibm.com/downloads/cas/9YBEK41O.

9. Robert Snow. 5 Key Predictions for Identity and Access Management and Fraud Detection. January 14, 2021. https://www.gartner.com/smarterwithgartner/5-key-predictions-for-identity-and-access-management-and-fraud-detection.

10. The Forrester Wave: Identity-As-A-Service For Enterprise, Q3 2021 by Sean Ryan with Merritt Maxim, Elsa Pikulik and Peggy Dostie, August 31, 2021.

https://reprints2.forrester.com/#/assets/2/108/RES176134/report.

11. AWS Business Applications. Масштабовані бізнес-додатки з оплатою по мірі використання, створені на AWS. https://aws.amazon.com/business-applications/?nc1=h_ls.

12. AWS Identity and Access Management. User Guide. https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf.

13. AWS Identity and Access Management (IAM). Apply fine-grained permissions to AWS services and resources. https://aws.amazon.com/iam/?nc1=h_ls.

14. AWS Single Sign-On. Centrally manage access to multiple AWS accounts or applications. https://aws.amazon.com/single-sign-on/?nc1=h_ls.

15. Manage IAM permissions. https://aws.amazon.com/ru/iam/features/manage-permissions/.

16. Кабанов Ярослав Вадимович. Технологія управління доступом користувачів до сервісів та ресурсів Amazon Web Services. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій. 27 жовтня 2021. Тези доповідей. С. 24 – 27. http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)